S. HRG. 114–257

PROTECTING TAXPAYERS FROM SCHEMES AND SCAMS DURING THE 2015 TAX FILING SEASON

HEARING

BEFORE THE

COMMITTEE ON FINANCE
UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

MARCH 12, 2015

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PUBLISHING OFFICE

20–033—PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON FINANCE

ORRIN G. HATCH, Utah, *Chairman*

CHUCK GRASSLEY, Iowa
MIKE CRAPO, Idaho
PAT ROBERTS, Kansas
MICHAEL B. ENZI, Wyoming
JOHN CORNYN, Texas
JOHN THUNE, South Dakota
RICHARD BURR, North Carolina
JOHNNY ISAKSON, Georgia
ROB PORTMAN, Ohio
PATRICK J. TOOMEY, Pennsylvania
DANIEL COATS, Indiana
DEAN HELLER, Nevada
TIM SCOTT, South Carolina

RON WYDEN, Oregon
CHARLES E. SCHUMER, New York
DEBBIE STABENOW, Michigan
MARIA CANTWELL, Washington
BILL NELSON, Florida
ROBERT MENENDEZ, New Jersey
THOMAS R. CARPER, Delaware
BENJAMIN L. CARDIN, Maryland
SHERROD BROWN, Ohio
MICHAEL F. BENNET, Colorado
ROBERT P. CASEY, Jr., Pennsylvania
MARK R. WARNER, Virginia

CHRIS CAMPBELL, *Staff Director*
JOSHUA SHEINKMAN, *Democratic Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL

COMMUNICATION

PROTECTING TAXPAYERS FROM SCHEMES AND SCAMS DURING THE 2015 TAX FILING SEASON

THURSDAY, MARCH 12, 2015

U.S. SENATE,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 10:02 a.m., in room SD–215, Dirksen Senate Office Building, Hon. Orrin G. Hatch (chairman of the committee) presiding.

Present: Senators Grassley, Crapo, Thune, Isakson, Toomey, Coats, Heller, Scott, Wyden, Cantwell, Menendez, Carper, Cardin, Bennet, Casey, and Warner.

Also present: Republican Staff: Kimberly Brandt, Chief Healthcare Investigative Counsel; Chris Armstrong, Deputy Chief Oversight Counsel; and Justin Coon, Detailee. Democratic Staff: Joshua Sheinkman, Staff Director; Tiffany Smith, Senior Tax Counsel; David Berick, Chief Investigator; and Daniel Goshorn, Investigator.

OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM UTAH, CHAIRMAN, COMMITTEE ON FINANCE

The CHAIRMAN. The committee will come to order.

The committee meets today to hear about growing criminal activity that is targeting taxpayers across the country. These criminal acts are perpetrated by thieves hiding behind telephone lines and computers, preying on honest taxpayers and robbing the Treasury of tens of billions of dollars every year.

This must stop, and we are here today to hear from some of the Federal and State officials on the front lines of the fight to catch these crooks and protect taxpayers. But first, I want to talk about one case in particular, and one very large number, by the way.

This is a hearing that is long overdue, as far as I am concerned. We will get into it. I have to apologize, as Senator Wyden is not here yet, but he is coming.

In this town, and especially right here on this committee, we often talk in terms of hundreds of millions, billions, or even trillions of dollars. Some joke about a number being referred to as "budget dust," even if that number has 9 or 10 zeroes behind it.

But let me tell you about a number that is truly stunning: $15,800. Now, that $15,800 was saved through hard work, sacrifice, and honest living. That is $15,800 saved for the down payment on a new house for a growing family. That $15,800 in savings was

wiped away by criminals who used fear, confusion, and intimidation as their weapons.

This is the story of the Degen family from Taylorsville, UT. I would like to play a news clip from KTVX, a Utah ABC affiliate, that tells their story. Can we do that?

[Playing of video.]

The CHAIRMAN. Well, that is just one family out of millions that have been targeted and thousands that have been victimized. This is just one scam. But make no mistake, taxpayers across the country are also facing identity theft in record numbers, account takeovers, and other criminal attacks.

Once again, we have to stop this. Taxpayers must be more aware of the risks and better protected from attack, and these criminals must be found and brought to justice. I look forward to the testimony from our witnesses on today's panel and to hearing more about how we can accomplish these goals.

Now, let me turn over the time to Senator Wyden for his opening remarks.

[The prepared statement of Chairman Hatch appears in the appendix.]

OPENING STATEMENT OF HON. RON WYDEN, A U.S. SENATOR FROM OREGON

Senator WYDEN. Thank you very much, Chairman Hatch. I very much appreciate the opportunity to work on these issues in a bipartisan way.

Colleagues, since the day that the IRS opened its doors, scam artists have been hatching up slick new ways of stealing taxpayer dollars from the Treasury. What is new is, the rip-off artists are now stealing Americans' identities and personally threatening them on an industrial scale, while directly robbing them of their hard-earned money. The fraudsters are constantly dreaming up new tactics, and then they milk them for all they are worth before they start getting caught. Then it is lather, rinse, and repeat, onto the next scam, always one step ahead of the law.

Today the committee will closely examine several of the fraudsters' latest strategies that are plaguing taxpayers. The one that is hitting Oregonians hardest is the fake phone call demanding money or personal information on behalf of the IRS. In fact, these calls were the number-one consumer complaint registered with the Oregon Department of Justice just last year. Not everybody knows that the IRS simply does not cold-call individuals, making demands or threats. So it is pretty clear from my vantage point, there is a lot more work to be done to defeat this scourge.

Given the sophistication of this criminal activity and the fact that a lot of it comes from overseas, this sure looks to me like an emerging type of organized crime. So the real question is, what is it going to take to root it out and get the bad actors on the sidelines—more prosecutions, stronger deterrence, more cops on the beat? What is the best way of getting the word out so that taxpayers are not tricked into surrendering their life's savings to some intimidating voice on the other end of the phone line?

But even if our people manage to avoid the phone calls, you can bet that the crooks find other ways to profit. Tax preparation soft-

ware has become the scammers' new fast lane. These sharks manage to acquire a taxpayer's personal data from the black market or hack into commercial databases, and then they file false returns electronically. The victims may not find out until much later in the tax season, and by then it is just too late. Already there have been thousands of reports like this in 2015. As we will hear today, some software vendors are not doing enough to help prevent fraud.

In my view, part of the challenge is getting the States' Internet tax services and the IRS on the same wavelength. They have to communicate and work together to make sure that the criminals cannot just, in a nimble fashion, slide from one jurisdiction to the next as they rip off more unsuspecting Americans.

Now, some taxpayers may choose to avoid software, but not even a paid tax preparer is guaranteed to be safe. In fact, many of them do not meet any standards for competence. There are far too many of these con artists out there willing and able to prey on the people who come through their doors. In some of the most offensive cases, they secretly falsify their victims' returns to boost the refunds and then they pocket the difference. Once the tax season ends, the crooks disappear from the storefronts they occupied, and there is no trace of where they have gone.

A few States, like mine, have rules in place to help shield the taxpayer from this kind of rip-off; most States do not. So Senator Cardin and I have introduced the Taxpayer Protection and Preparer Proficiency Act at the beginning of this Congress to give all Americans the security they deserve. Our colleague Senator Nelson is also a leader on this issue of keeping taxpayers safe from identity theft and fraud, and all of us wish, as I indicated to Chairman Hatch, to work on this in a bipartisan way.

The bottom line is, there is no end to the ingenuity of the con artists, so my hope this morning is that we will get some fresh ideas for catching up to this wave of fraud and stopping it. Obviously, it cannot come soon enough. We have a distinguished panel here today. I am especially pleased that Ms. Ellen Klem, the Director of Consumer Outreach and Education in the Oregon Attorney General's office, is here. My thanks to Ms. Klem, and to all our witnesses.

Mr. Chairman, I look forward to working with you and our colleagues on this in a bipartisan way.

The CHAIRMAN. Well, thank you, Senator Wyden.

[The prepared statement of Senator Wyden appears in the appendix.]

The CHAIRMAN. Our first witness today is Acting Assistant Attorney General Caroline Ciraolo of the Tax Division of the U.S. Department of Justice. Ms. Ciraolo was appointed Principal Deputy Assistant Attorney General and Deputy Assistant Attorney General of Planning and Policy of the Tax Division in January of this year. Prior to that, she was chair of the Tax and Litigation Group at Rosenberg, Martin, Greenberg in Baltimore.

Ms. Ciraolo, we welcome you to the committee, and we look forward to hearing your testimony.

STATEMENT OF CAROLINE CIRAOLO, ACTING ASSISTANT ATTORNEY GENERAL, TAX DIVISION, DEPARTMENT OF JUSTICE, WASHINGTON, DC

Ms. CIRAOLO. Thank you, Senator.

Chairman Hatch, Ranking Member Wyden, and members of the committee, thank you for the opportunity to appear before you to discuss the Department of Justice's efforts to combat identity theft and tax refund fraud.

The Department greatly appreciates the commitment that this committee has brought to this very important issue. Combating the theft of personal information to file fraudulent tax refund claims is a top priority for both the Tax Division and U.S. Attorneys' offices across the country. Your efforts to bring attention to this growing and insidious crime will help educate taxpayers about the importance of detecting and reporting identity theft and fraud. Today's hearing also sends a strong message that the government is determined to identify and prosecute the individuals behind these schemes and, in doing so, will bring all its resources to bear.

The Department's Tax Division, which I had the honor and privilege of leading as Acting Assistant Attorney General, has one purpose: to enforce the Nation's tax laws fully, fairly, and consistently through civil litigation and criminal prosecutions. Our close working relationships with IRS Criminal Investigation, TIGTA, the U.S. Postal Service, the FBI, the U.S. Attorneys' offices, and other Federal, State, and local law enforcement partners, continue to enhance the government's ability to respond quickly, efficiently, and forcefully to often-changing patterns of criminal conduct.

Stolen identity refund fraud, or SIRF, is an example of this type of challenge. In SIRF crimes, offenders steal Social Security numbers and other personal information. They file tax returns early in the filing season, showing a false refund claim, and then have the refunds electronically deposited to a bank account, loaded on prepaid debit cards, or mailed to an address where the wrongdoer can access a check.

SIRF crimes often involve multiple offenders at various levels in a conspiracy, and frequently involve employees with access to databases containing large volumes of personal information. SIRF crimes often hit the most vulnerable members of our society, like Melissa and Brendan Degen. These include, but are certainly not limited to, the elderly, the hospitalized, students, and members of our military deployed overseas. While the IRS will make good on any refund due to the taxpayer, there are inevitable burdens and delays while the matter is addressed, and the victims often experience a profound sense of violation. Moreover, we are all victimized by a loss to the U.S. Treasury.

SIRF crimes require immediate action to prevent enormous harm to the American public. To this end, the Tax Division expedites its review procedures in SIRF cases, and has issued directive 144, which delegates to U.S. Attorneys' offices, among other things, the authority to initiate tax-related grand jury investigations in SIRF matters and to charge those involved in SIRF crimes by complaint without prior authorization from the Tax Division. The collaborative efforts of the Tax Division and its law enforcement partners have strengthened the response to this crime. Through December

31, 2014, the Department prosecuted more than 1,400 individuals, and courts are imposing substantial sentences.

To further leverage the information gained from each investigation, in February 2014, the Assistant Attorney General of the Tax Division created a SIRF Advisory Board, consisting of experienced SIRF prosecutors. The board works to develop and implement a national strategy to ensure consistent and effective nationwide enforcement and prosecution of SIRF crimes.

For example, the board conducts training sessions for fraud analysts at the IRS Scheme Development Centers. The board provides training and resources to prosecutors across the country, and it works with U.S. Attorneys' offices to develop local task forces.

These initiatives enable prosecutors and law enforcement agencies to work together to identify schemes and to pursue the most culpable offenders while providing the IRS with real-time information that can be used to improve its filters and stop the issuance of fraudulent refunds. The prosecution of SIRF crimes is a national priority, and, together with our law enforcement partners, we will continue to look for the most effective ways to punish the offenders and bring this conduct to an end.

Thank you again for this opportunity to provide the Department's perspective on this issue, and I look forward to answering any questions you may have.

The CHAIRMAN. Well, thank you so much.

[The prepared statement of Ms. Ciraolo appears in the appendix.]

The CHAIRMAN. Our next witness is Timothy Camus, the Deputy Inspector General for Investigations at the Treasury Inspector General for Tax Administration, or TIGTA. Mr. Camus has served at TIGTA and TIGTA's predecessor, the Internal Revenue Service's Inspection Service, for over 23 years. He has a long career of having successfully investigated cases of domestic terrorism, bribery, and fraud affecting the IRS.

We certainly welcome you, Mr. Camus, and we look forward to taking your testimony at this time.

STATEMENT OF TIMOTHY P. CAMUS, DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, DEPARTMENT OF THE TREASURY, WASHINGTON, DC

Mr. CAMUS. Thank you, Chairman Hatch, Ranking Member Wyden, and members of the committee. Thank you for the opportunity to testify on the topic of tax schemes and scams during the 2015 filing season.

By raising public awareness about criminals' efforts to swindle honest Americans out of their money, we may prevent the next person from becoming a victim, which is a very good thing. Each year, the IRS compiles what it sees as the dirty dozen tax scams on its website. Many of these schemes peak during the filing season as people prepare their returns or utilize the service of paid preparers. My statement today briefly outlines the top schemes and scams currently affecting taxpayers, as they have proven to be surprisingly effective ways to steal money, in many cases before the victim even realizes they have been scammed.

The first scam is the phone impersonation scam, which landed on the top of the dirty dozen list this year. It is the largest and most pervasive impersonation scam that we are aware of, and it has claimed thousands of victims in every State represented on this committee.

Here is how it works. The intended victim receives an unsolicited phone call from a person claiming to be an IRS agent. The caller, using a fake name, tells the victim a made-up badge number and claims that they owe tax and that they are criminally liable for some amount owed. The callers may even know the last four digits of the victim's Social Security number. They then threaten the victim by stating if they fail to pay immediately, the victim will be arrested or face other criminal sanctions, such as losing their driver's license.

I myself received one of these calls at my home on a Saturday. TIGTA has received over 366,000 reports of these calls, averaging between 9,000 and 12,000 calls coming in to my agency each week. As of March 9, 2015, over 3,000 individuals have been victimized by this scam, by paying a total of $15.5 million, or an average of $5,000 per victim.

The highest reported loss by one individual was a staggering $500,000, and in one particularly sad story, a member of this committee forwarded a letter to us from a constituent whose close relative suffered a tragic death after receiving harassing phone calls from these scammers.

To help educate taxpayers, we are reaching out via the media in conjunction with the IRS and the Federal Trade Commission, as well as providing testimony to this committee, in hopes of eliminating this type of abuse and preventing other vulnerable individuals from becoming victimized.

Another ongoing scam I would like to highlight involves using the story that the victim has won a lottery. This is a continuation of an old scam. It starts with an e-mail or a telephone call out of the blue declaring that the victim has won the lottery, but, in order to collect the winnings, they must first pay the tax to the IRS. The lottery scam often, but not always, originates from outside of the United States. In the end, the victims pay the money, but they never receive any lottery winnings.

Just as serious as these scams is the risk of taxpayer refund identity theft. The IRS has made improvements in its identification of identity theft returns before fraudulent tax refunds are released, but continued attention is needed to effectively combat this crime. For example, the IRS still does not have timely access to third-party income and withholding information. Most of this third-party information is not received by the IRS until well after the taxpayers begin filing their returns.

The deadline for most information returns with the IRS is March 31st, yet taxpayers began filing their returns this year on January 20th. This gap in time prevents the IRS from conducting validity checks. Of course, legislation would be needed to accelerate the filing of the information returns.

The IRS has taken steps to effectively prevent the filing of identity theft tax returns by locking the tax accounts of deceased indi-

viduals to prevent others from filing a return using the departed's name or Social Security number.

For processing year 2014, the IRS rejected over 338,000 e-filed returns and stopped nearly 16,000 paper-filed returns through the use of these locks. Just 11 days after the filing season this year began, the IRS reported that it had prevented the issuance of more than $2 million in fraudulent refunds as a result of these filters.

Other schemes such as prisoner fraud, unscrupulous tax preparers, and phishing scams are discussed in depth in my written testimony. Much work is being done on multiple fronts to address these criminal activities. We hope this work will reduce or eliminate their impact on taxpayers.

Chairman Hatch, Ranking Member Wyden, thank you for the opportunity to share my views. I look forward to questions.

The CHAIRMAN. Thank you so much.

[The prepared statement of Mr. Camus appears in the appendix.]

The CHAIRMAN. I am going to turn, briefly, to Senator Coats to introduce our next witness.

OPENING STATEMENT OF HON. DANIEL COATS, A U.S. SENATOR FROM INDIANA

Senator COATS. Mr. Chairman, thank you very much. I thank you for inviting our Indiana Department of Revenue Commissioner Mike Alley to testify today.

Thanks to the leadership of our Governor Mike Pence and Commissioner Alley, our Department of Revenue developed a plan that stopped $88 million in attempted identity theft in the last filing season. This involved 78,000 fraudulent returns and 12 percent of all the refund dollars that were requested.

The effort to do that, as Mr. Alley will explain, cost the State $8 million. The return on investment was $88 million. Compared with some of the things we do around here, which are usually the opposite—spend $88 and get $8—we spent $8 and got $88 back and saved a lot of taxpayers from this fraud, and we are currently bringing the needed savings to our State.

Mr. Alley, Commissioner Alley, brings a wealth of private-sector experiences to his job. He has worked for decades in leadership positions in the banking industry. He is a CPA. He has started businesses, so he understands, first-hand, how important the customer service role is for the Department of Revenue.

Again, Mr. Chairman, I thank you for inviting Commissioner Mike Alley to testify this morning and look forward to his testimony.

The CHAIRMAN. Great.

STATEMENT OF HON. MIKE ALLEY, COMMISSIONER, INDIANA DEPARTMENT OF REVENUE, INDIANAPOLIS, IN

Commissioner ALLEY. Thank you, Senator Coats.

Chairman Hatch, Ranking Member Wyden, and committee members, thank you for inviting me to discuss this important topic with you today. On behalf of Governor Pence and the citizens of Indiana, it truly is our honor to be here and share our story.

I would like to share really three points with you today: the first, the nature of the problem and the overall breadth, which we have

already heard here today is significant; the steps that Indiana has taken and the lessons we have learned; and then recommendations to more fully and effectively address this epidemic problem.

Tax refund fraud is one of the most lucrative platforms for criminals to monetize the value of stolen identity information, and the advent of electronic filing and processing has only enhanced the ability of criminals to utilize economies of scale in filing large volumes of fraudulent returns at nominal cost.

As Senator Coats indicated, in 2014, 12 percent of the total refund dollars that were requested from Indiana were found to be fraudulent. Fortunately, we were able to stop them. They represented 78,000 fraudulent returns that we stopped that contained manufactured or stolen IDs, and again we saved the State $88 million in the process.

It is still early in the 2015 filing season, but we are already seeing a dramatic increase in the use of valid IDs which have been stolen. With the increase of the reported successful hacks all across the United States of U.S. companies, we believe the availability of valid stolen IDs has never been greater, and the fraudsters have clearly upped their game, and we must do the same.

Second, let me share with you what we have done here in Indiana. In 2012, we realized that we were suffering substantial losses from refund fraud. Accordingly, we worked with Governor Pence and his team to effectively identify a program that we could begin building. We knew that we needed to make significant systemic modifications, and we needed to do it before the next filing season. Our staff reached out to fellow States through the Federation of Tax Administrators and also our partners at the IRS, to see if there were some ideas we could borrow and implement rapidly. The response was very supportive, though we noted partial solutions and fragmented efforts across the group.

With strong support from Governor Pence, we initiated a pilot program to screen all returns for suspicious identities. This program used LexisNexis®, a third-party commercial vendor, to screen returns and note identity theft information such as name, address, Social Security number, and other identifier information.

We processed those returns. When they proved to be suspicious, we withheld those, and sent a confirmation letter to those taxpayers to have them confirm their identities. Again, this had a dramatic impact on our ability to recognize fraudulent identities and stop those refunds.

The identity confirmation quiz is only a part of a larger process. It became very clear in the beginning that the Department would need to make some systemic changes by making significant investment in both staff and technology, and, further, we needed to change our approach to how we deal with fraud.

For the 2015 filing season, we have continued to make enhancements. We have implemented some new pre-filter processing platforms that include a decision matrix that will allow us to better identify those valid IDs. We have also defined greater expectations from our certified software vendors as to the information they will provide to us and the level of fraud that they send our way.

We are still battling this problem, but a few key lessons have been learned. First, it must be a strategic priority. Identity theft

and refund fraud are here to stay, and we have to address them. It requires a fiscal investment in leadership, staff, technology, and third-party resources.

Second, collaboration. No one has all the answers, and we cannot solve this problem by ourselves. Sharing data, best practices, and experiences among all of the revenue agencies across the States, as well as the Federal Government and software vendors, is going to be important. Having access and ability to communicate on a timely basis is critical. We have to develop some targeted solutions. Fraudsters will continue to change their approaches, and we have to stay ahead.

Finally, I would just note that the pre-paid debit card is an issue that I think needs to be addressed. It is a preferred tool of fraudsters in receiving their refunds. We found that over 50 percent of those returns with pre-paid debit cards are fraudulent.

In terms of some recommendations on things we can do, we consider that the solution really encompasses a three-legged stool concept which notes that the States, the IRS, and software vendors each represent a significant and important leg of the stool. Each has unique data, perspectives, and capabilities that the system as a whole requires in order for us to make better decisions.

The IRS is certainly in a great position to help us manage highly sophisticated fraud. States must work more collaboratively together. Finally, software vendors also have great information and can be helpful in sharing their intelligence.

In conclusion, I just want to summarize that, first, this problem is here to stay, and we have to address it. Second, collaboration and sharing of information among the IRS and the States, reducing some of the barriers to our ability to share anonymous aggregate information, is critical. Third, we have to make the investments. As Senator Coats noted, we made an investment that yielded over a ten-times return, and I am confident providing that continued investment is the only way that we can get out ahead of this and beat it.

On behalf of Governor Mike Pence and the citizens of Indiana, thank you for allowing us to share our story. I look forward to trying to answer any questions you may have, but thank you for allowing us to be here.

The CHAIRMAN. Well, thank you. Thank you, Senator Coats and Commissioner Alley. We appreciate you making an effort to be here.

[The prepared statement of Commissioner Alley appears in the appendix.]

The CHAIRMAN. Now I am very pleased to introduce our next witness, Commission Chair John Valentine of the Utah State Tax Commission. Chairman Valentine was a member of the Utah State Senate, where he served with distinction from 1998 until his confirmation as Tax Commission Chair in September 2014.

Prior to that, he was in the Utah House of Representatives, and was also an attorney in private practice. Chairman Valentine, we are really grateful that you have taken time out of your schedule to be with us today. I want to thank you for coming to Washington during the filing season and joining the hearing this morning. So, we appreciate all of you being here.

STATEMENT OF HON. JOHN L. VALENTINE, CHAIRMAN, UTAH STATE TAX COMMISSION, SALT LAKE CITY, UT

Mr. VALENTINE. Thank you very much, Chairman Hatch and Ranking Member Wyden. Thank you also for giving us this time.

Esteemed members of the committee, I am here to discuss ways to reduce the tax frauds that we are seeing envelop this country. There are four issues that you really ought to consider: (1) strengthening information sharing between the IRS and the States; (2) stricter regulation of the financial industry as it relates to prepaid debit cards; (3) regulating the practice of applying refunds to payment of fees for filing services, a practice sometimes called in the industry "refund transfers"; and (4) requiring third-party filing services to tighten front-end security by using multi-factor authentication and other measures to secure data from unauthorized disclosure and identity theft.

Prior to the commencement of the 2015 filing season, Utah installed a state-of-the-art computer software system to identify potentially fraudulent returns. On January 20th of this year, the Utah Tax Commission opened filing of income tax returns and deployed this system. As we began to process returns, our system started sending out error notices that indicated that there were fraudulent returns.

We then followed up with verification letters of the suspicious returns to the taxpayers. Within 10 days after opening the filing season, we began receiving calls from taxpayers saying, "We have not filed our returns yet." We initially thought that these were isolated incidents, but, as the week progressed, it was clear that they were not.

We found several factors that were common in all of these calls: (1) the returns had the direct deposit information changed from the previous year's bank account to a pre-paid debit card; (2) the returns contained routing and account numbers that differed between the Federal returns and the State returns; and (3) most of the returns appeared to have the exact 2013 return data populated in the 2014 return.

The next issue we found was common was that the address on the returns was the same as the address on the 2013 return, even when there was an error in the address. Finally, since most of the filings were made through one vendor, it appeared that something in their process was compromised.

After communicating with that vendor and notifying other States of what we were finding, we talked with the Internal Revenue Service and said, "We think there may be a compromise of the MEF system," that is the Modernized Electronic Filing system.

The accounts in question that we were able to identify were immediately sent to the Ogden Service Center. Thirty-one returns in that first week were confirmed suspicious. We asked them in a phone conversation to confirm on their side. We are still waiting to hear from them.

Many have asked what action was undertaken by the State of Utah when it discovered this attack. In short, we hurried. We stopped all refunds until we could get our arms around it. During that first week, we found five different fraud schemes, four of which were ones we had seen before—they are institutions, they

are preparers. But one was a new one, and the new one involved someone who had actual tax returns—not just identity theft, but tax returns from the prior year.

Now, as we continued to prevent the outflow of fraudulent refunds, we found great difficulty in determining the nature of the financial institution and the account information. Specifically, we found that there was no uniformity in numbering to determine traditional debit cards from traditional bank accounts. In other words, we could not tell whether we were refunding to a pre-paid debit card or whether we were refunding to a legitimate bank account. There is an easy fix on this one. The easy fix is to require the financial industries to have identifier numbers in the routing number or in the account number to identify the account as a pre-paid debit card. We do that already with checking accounts and savings accounts; we do not do it with pre-paid debit cards.

While we progressed through the investigation, we found a practice that enables fraudsters to perpetrate fraud without having anything at all at risk: the refund transfer. Here is how it works. The fraudster is allowed to deduct the third-party filing fees from the refund, the third-party filing fee gets paid, the fraudster receives the cash, and the State of Utah is out the money.

Finally, we found third-party filing services often lack front-end identity security measures. Quality firewalls need to be installed by third-party vendors, both for the IRS and for the State Tax Commissions.

Thank you, Mr. Chairman. Thank you, Ranking Member Wyden.

The CHAIRMAN. Well, thank you. We appreciate your testimony.

[The prepared statement of Mr. Valentine appears in the appendix.]

The CHAIRMAN. Finally, we welcome Ellen Klem from the Office of the Oregon Attorney General. Ms. Klem serves as the Director of Consumer Education and Outreach at the Attorney General's Office and works to protect Oregonians from financial scams, including the types of scams and schemes we are talking about today. So we are happy to welcome you here as we have the others, and we look forward to taking your testimony.

STATEMENT OF ELLEN M. KLEM, DIRECTOR OF CONSUMER OUTREACH AND EDUCATION, OFFICE OF THE ATTORNEY GENERAL, OREGON DEPARTMENT OF JUSTICE, SALEM, OR

Ms. KLEM. Thank you, Chairman Hatch and Ranking Member Wyden. It is an honor to be here today and share my expertise and experience with you.

Every day I hear stories from Oregonians about a wide variety of frauds and scams. Lately, these stories have focused almost exclusively on the IRS imposter scam. That is because, as Senator Wyden mentioned earlier, in 2014 this scam topped Oregon's list of consumer complaints. Last year, we received more than 1,300, nearly twice the number as the next highest category. What is worse, these victims reported losses to us totaling more than $75,000, and we know from testimony presented here today that that number is just the tip of the iceberg. That is why I am here today to tell you the story of two of those victims and to talk a little

bit about what the Oregon Attorney General is doing to prevent this from happening to others.

The first story is that of a woman I will refer to as Diane. In August of 2014, she lost $15,000 to an IRS imposter scam. This is the largest individual loss reported to the Oregon Department of Justice in 2014. Like many other victims, she received a message on her answering machine from a man claiming to be from the IRS, directing her to call him back at a phone number with a 202 area code. She returned the call, and the person who answered read her an affidavit for her arrest, threatened her with a fine of $25,000, 18 months in prison, and told her she would be arrested later that day if she did not pay. Diane was terrified. She pleaded, she begged. The scammer said he could settle the matter, but only if she paid $15,000 by purchasing a series of pre-paid money cards. Diane made the only choice she thought she had. She complied with the request, and she was out $15,000.

Individuals like Diane who send money to the scammers are not the only victims of imposter scams. In September of 2014, I was contacted by Marissa Phillips, a small business owner whose employee, Linda, had fallen victim to an imposter scam. After sending a very small amount of money to the scammers, Linda quickly realized she had been had and stopped answering her phone. But the scammers kept calling. When it was clear they were not going to get a hold of Linda at that phone number, they began calling Marissa's small business, a business that provides in-home care services for seniors and persons with disabilities. When Marissa called me a few days later, she told me the scammers had called her business at a rate of 100 phone calls per minute for 20 minutes straight, and all of these calls prevented her from providing help to those who actually needed it, the seniors, their families, hospitals, doctors, and other staff. Ultimately, Marissa was forced to change her business's phone number and all of its accompanying marketing materials.

Thankfully, not everyone in Oregon who receives a phone call from an IRS imposter falls victim to the scam, and I would like to think that is because we have been working very hard to educate all Oregonians, especially our most vulnerable. The Oregon Attorney General has several educational tools aimed at scam prevention, because she and I both know that well-informed Oregonians are much more likely to recognize fraud and less likely to become victims if they are educated.

We also know that these scams can be very hard to track and prosecute. The Oregon Attorney General also has invested in strong partnerships with Federal, State, and local governmental entities and officials, tribes, community organizations, advocacy groups, and members of the media. Through these partnerships, we are able to share complaints, coordinate investigations, and disseminate information to the public. Our partners give us a stronger voice to share information and keep Oregonians like Diane, Linda, and Marissa safe.

This concludes my testimony. Again, thank you, Chairman Hatch, and thank you, Senator Wyden, for the opportunity to share these stories with you today.

The CHAIRMAN. Well, we want to thank you and all the witnesses here today. My gosh, I think a lot of people are going to be very surprised at how this is ballooning in our country.

[The prepared statement of Ms. Klem appears in the appendix.]

The CHAIRMAN. Let me turn to you, Commissioner Valentine. I want to thank you again for coming all the way back here to testify in the midst of filing season. I really applaud the innovative approaches that you are taking, that you and other State commissioners like Commissioner Alley are taking as well, to protect our taxpayers and to stop criminals.

Now, in your testimony, you mentioned that you would like to strengthen information sharing between the IRS and the States. I would really appreciate it if you would elaborate a little bit more on that idea, just to explain what kind of information would be useful to you and what information you could provide to the IRS that would perhaps be useful to them. If you have any suggestions about how the Finance Committee could help facilitate the sharing of information, I would also like to have you comment on that, if you would care to.

Mr. VALENTINE. Thank you, Mr. Chairman. There are actually a couple of places that are kind of rub points. Let me say this as the background though: we have a great working relationship with the IRS, especially the agents we deal with. The Memorandum of Understanding that we have with the Service allows us to share information. The trouble is, it is not being shared in real time. The information is very, very much delayed. Sometimes we are not getting the information that we could use in a timely fashion to be able to look at the returns as they are coming in.

One of the things that the Senate Finance Committee may consider is the idea of moving up the filing deadline for the W–2s for employers. As I think Senator Wyden indicated, we have a problem. Right now, the W–2s go out to the individuals on the 31st, but we have a big gap, because the employers do not have to have them out until March 31st. So we have a 2-month gap.

States are under a lot of pressure, as is the Federal Government, to make the refunds. This is the people's money; they have overpaid it. Yet, we cannot give them the refund without knowing for certain that the right person is getting the refund. That gap is a big problem for us, and that one would help a lot.

Another one is for the Senate and the House to be able to really encourage the IRS to have a more formalized sharing of information. I gave you the one example of the 31 returns we submitted 6 weeks ago. They should be able to respond pretty quickly on something like that. We had identified them as fraudulent returns, we confirmed with the taxpayers that the returns had not even been filed, and yet we still cannot hear back in real time. Those are the kinds of things that I think could really help.

The CHAIRMAN. Well, thank you very much.

Mr. Camus, let me ask you this. I want to thank you and the Inspector General as well for all of your efforts to catch these criminals and educate the public about these types of scams.

In my opening statement, I showed the video about the Degen family. The same criminals who targeted them are likely out there at this very minute targeting other Americans. Can you pledge to

me that your office is doing everything in its power to track them down and stop them? Can I have that commitment?

Mr. CAMUS. Sir, you more than have that commitment. The men and women who work at the Treasury Inspector General for Tax Administration are working day and night on this crime, and we are partnering with other law enforcement agencies as well. It hurts us when these victims are victimized as described here.

We instruct our agents that when they run into a victim or they hear from a victim who has actually lost money, we need to spend time with those victims, hear their stories, and attempt to get as much information as we can. We have a very aggressive, ongoing investigation at this time, and I would hope that in the very near future I could come and describe to you the successes of that investigation.

The CHAIRMAN. That is great. Another scam that particularly worries me is the stolen identity refund fraud. A recent GAO report calculated that the IRS paid at least $5.8 billion of fraudulent refunds to identified thieves in 2013. Now, this type of fraud is usually not detected until the refund has already been issued. As a result, the government must attempt to recover funds that have already been disbursed to a criminal, which is no easy task. It would be better if we could detect more of this fraud before payments are made.

Do you have any suggestions about how TIGTA and the IRS can detect this type of fraud earlier and stop fraudulent payments from going out the door?

Mr. CAMUS. Well, as noted in opening statements by the witnesses and the committee members, one of the challenges is that criminals are out there watching the Internal Revenue Service. They realize that $3.1 trillion goes through the IRS on an annual basis, $374 billion in refunds. It is a very ripe target for them. So, as the IRS continues to try to advance its filters in response to new approaches to the fraud, the criminals change, because it is such a lucrative environment.

Our audit staff continues to look at the filters that the IRS has in place and comment and recommend additional or improved filters. We have seen improvement in some of them, but it continues to be a major challenge to keep up with the criminal enterprises.

The CHAIRMAN. Well, thank you.

Senator Wyden, we will turn to you.

Senator WYDEN. Thank you very much. This has been a superb panel, Mr. Chairman. Ms. Klem, thank you for the wonderful work that you are doing in our State, particularly for older people. I think you know, those are my roots with the Gray Panthers, so I am really glad that you are out there on that beat. It is incredibly important.

I want to ask you, Mr. Camus, about this question of the foreign governments, because it seems to me—and you mentioned it in your testimony—it is clear that the phone scams, a lot of them, are originating overseas. It looks to me like this is essentially an emerging form of organized crime. You are conducting an investigation, and I recognize that there are some things you cannot say, but let us talk a little bit about some of the things that we ought to be looking at from a policy standpoint.

First, there is the question of whether we ought to be initiating efforts in terms of work with foreign governments and what they can do to assist with this. The second is, what is the appropriate role for local law enforcement, because you can go after the money runners who collect the payments. In other words, the rip-off artists are overseas, but they are going to need money runners to collect the payments.

So let us start with those two, and there may be other opportunities. I know we have strike forces in terms of Medicaid, these interagency forces. But tell us a little bit—nothing that will compromise your investigation—about what we can be looking at that will give you more tools to fight particularly the rip-off artists who have done so much damage from overseas.

Mr. CAMUS. Thank you so much for the opportunity. Of course, the challenge when we are dealing with these attacks being launched offshore is, first of all, getting our hands on these people. As you pointed out, Senator, the agreements or working relationships we would have with various foreign governments can create issues there, and we would ask for help with that.

The problem we are seeing now is that, because there has been money paid, we are seeing other spin-offs of this crime. So, although we are focused and we think we know where it originated to start, we are now starting to see indications that other criminals have ripped off the original idea, and now they are launching these types of attacks.

So it continues to be a challenge, but I think we are onto something. But it would certainly be something we could use some help with on down the road as far as getting our hands on a foreign national and bringing him to justice in the United States for a white-collar crime.

Senator WYDEN. Without compromising the investigation, can you tell us a little bit—you said there were some problems in working with the foreign governments. Can you just give us a little bit of a sense of what those are?

Mr. CAMUS. Well, as you could imagine, in the world today, not all foreign governments would feel sorry for the United States, with our citizens and the integrity of our financial systems suffering these types of scams. It is one of the reasons my agency takes this crime so seriously, because it impugns the integrity of the Internal Revenue Service. So there are those out there who do not feel bad for the United States and are not necessarily interested in helping us bring these types of criminals to justice, sir.

Senator WYDEN. Let us move on to the Anthem case, because this is one that really shows the industrial scale of these incredible rip-offs, something like 80 million people affected by cyber-ID theft. They are one of the biggest health insurers in the country. They have indicated now that 80 million Americans may have been hacked, opening the way to misuse of this data, certainly in terms of fraudulent health claims, but also this criminal enterprise we are talking about today with ID theft, including tax fraud.

I have raised this question with the Inspector General in the past. It seems to me that blocking this type of tax fraud increasingly is going to fall on the shoulders of tax collectors, both the IRS and the States. So I would be interested in the panel's rec-

ommendations on what else we need to do to give you the tools to fight ID theft from cyber-attacks. So, any of you who would like to get into it——

I saw all the State officials already nodding their heads. Why don't we hear from Indiana first, just to keep things in the center. I always like to get to the center before the far right and the far left go at it. [Laughter.]

Commissioner ALLEY. Thank you, Senator Wyden. Well, in fact, anecdotally we are seeing a significant increase in the number of valid stolen IDs in Indiana, with Anthem being based in Indiana. So we already are seeing the impact of that.

I think many of the steps that corporations all across the country are having to take involve more multi-faceted authentication in terms of accessing their systems. I think many companies have not invested adequately to prepare themselves for that and it will leave them vulnerable, so I think that is one key thing that corporate America, and all of us even at the governmental level, need to focus on.

In terms of what we can do as a group, I think it goes back to that three-legged stool I spoke about earlier. It is making sure that we are sharing those information elements more readily and more rapidly. As Commissioner Valentine indicated, oftentimes we do get a great deal of information that we share with one another, but it is not on a timely basis.

I would also really like to see the IRS take a greater leadership role in terms of driving many of the standards or expectations. We have 50 States, and many of them do have taxing mechanisms and Departments of Revenue all doing disparate things. If we could have the IRS help us to bring everybody together to establish a coordinated, collaborated set of standards and expectations from our software vendors, from financial institutions as well, I think that could do a great deal to bring everybody together on the same platform.

Senator WYDEN. My time is up. That sounds too logical, so we will have to pursue it. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Senator Thune, your turn.

Senator THUNE. Thank you, Mr. Chairman. Thank you and Ranking Member Wyden for holding this important hearing. Thank you to our panelists for being here and for their willingness to testify.

I think every taxpayer ought to feel confident knowing that their personal tax information is secure when they file it with the IRS and that there will not be a false return fraudulently filed in their name.

I think we all know and have seen the devastating impact that tax-related identity theft can have on a family's financial well-being, so I appreciate the committee's interest in the subject, and I hope we are able to move legislation forward in Congress.

One measure for preventing tax-related identity theft that has been recommended by a number of commentators is for the IRS to verify information from third parties, such as the Social Security Administration. I am wondering what your thoughts are about how much fraud that would prevent, and are there any potential down-

sides to that approach? I would just throw that open to anybody who would like to comment on that.

Mr. Camus?

Mr. CAMUS. Sir, thank you. Our auditors look at that on a regular basis, and they are in the middle of doing some audit work right now. But generally speaking—and Mr. Valentine pointed it out—the fact that the IRS does not have in its automated system a W–2, for example, to match at the same time the taxpayer files a return, that inhibits their ability to do a very simple validity check before issuing a refund.

There is a great expectation to get the taxpayers a refund as soon as possible, because after all it is the taxpayer's money. So anything that we can do to increase the timeliness or to get the time the taxpayer can start filing their return—which this year was January 20th—to jive with the time theSocial Security Administration has the W–2 information, which really is not due until March 31st, I think that would be a big help.

Senator THUNE. All right. Does anybody else want to comment on that subject, or are there any downsides to that approach?

Mr. VALENTINE. I am not aware of the downsides, other than the fact that there would be more information being transferred and places for it to be leaked out.

But there are actually three areas that can really affect the fraud issues. The one is on the front end, which is the authentication issue, which is what you are speaking of. The next one is in the discovery phase, which is those transfers of information that occur back and forth between the various different tax agencies. The third one is the method that you use to pay. That is why the suggestions that I made really tried to affect all three of those. Any one of those is helpful, but you need to approach it, I think, in all three areas. If you do that, then you can really have a better chance of actually cutting the frauds down.

Senator THUNE. All right. Thank you.

It has been a number of years since Congress enacted a Taxpayers' Bill of Rights. When a taxpayer has a fraudulent return filed in his name, is the recourse with the IRS sufficient?

Mr. CAMUS. Again, our audit staff looks at that: what the victim experience is like when they contact the Internal Revenue Service, what type of service they get, and what the IRS does to help the taxpayer victim. We are continuing to look at that and audit and recommend changes or improvements in that program.

Senator THUNE. And I was going to say, are there additional measures that ought to be considered to make it easier for individuals who find themselves in that situation to get the assistance that they need?

Mr. CAMUS. Of course, it is a very traumatic issue for the victim. Anytime anybody's identity has been compromised, they are very, very upset. Again, I am not ready to comment on where we are and what we are doing, but I do understand from our auditors that there has been improvement, and they continue to work and look to make that experience better for the victim.

Mr. VALENTINE. Senator, I can tell you, in the State of Utah we have a Taxpayer Services Division which focuses exactly on the issue that you are raising, and that is, when someone claims that

they have a fraudulent return, they have to have a way to be able to process it quickly without having to go through the whole State bureaucracy.

We have done that with our Taxpayer Services Division in a quiz letter that we send out to be able to authenticate that the person who is calling us is in fact the right person. That kind of thing may be something the Service could consider as well, to really have a way to expedite a particular complaint of identity theft.

Senator THUNE. Just very quickly, there have been recent breaches involving TurboTax that have made national news. Is there a reason why TurboTax has experienced this but other electronic providers of tax service have not? How preventable is this?

Commissioner ALLEY. I am not so sure that others have not also been impacted. I think perhaps we have realized it and directly identified the particular breaches that occurred with the one vendor—which they have taken additional steps to try to mitigate—but I think we are finding in Indiana that it is not just TurboTax that has been impacted by this. I think the fraudsters are moving. I mean, they move with great agility. As they impact one and have success and those doors close, then they readily move to another open door. So I think it is a systemic issue and really broad across the entire industry, not limited to any particular vendor or party.

Senator THUNE. Thank you. Thank you, Mr. Chairman. Thank you all very much.

The CHAIRMAN. Senator Warner?

Senator WARNER. Well, thank you, Mr. Chairman. Thank you for holding this hearing. We all have stories from our constituents. We hear the same kind of stories in Virginia.

Mr. Chairman, one of the things that I think we could do that comes to my attention is—Senator Ron Johnson and I have some legislation on this—the IRS currently interprets the law as saying that if they find out that you have been the victim of identity fraud, they do not even have to tell you as a citizen that you are the victim of that fraud. They do not have to notify law enforcement. So, on the notion of whether I believe they could do it administratively, we have written to them.

Perhaps you and the ranking member writing them might shake them up a little bit more. But if we cannot get at it administratively, one step that we could take would be making sure that the IRS is actually a partner in this effort in identification. When it comes to their attention that somebody has been a victim of identity theft, we notify the victim and law enforcement. I think we see some nods from the panel there. Again, the numbers are huge, as you pointed out in your testimony: $5.8 billion in 2013.

A second item that I think we ought to consider is—and this is something I have been working on in the Banking Committee; I know Senator Carper walked in briefly—some level of mandatory data breach reporting. It is a very gray and developing area.

When, particularly on the retail side, we have a data breach—we have seen countless indications of data breach, but there is no obligation, there is no standard yet, about when a company needs to report this information. I think there needs to be such a standard.

One of the things we have urged from the Banking Committee side is that—this is an area where there is a lot of finger-pointing between the retail sector and the financial sector, and rather than creating another interchange battle, we should try to have the financial sector and the retail sector actually collaborate better. I am going to get to a question here.

It would seem to me as well, and one thing that I would like the panel's comments on is, is there not a way, either through the IRS or in collaboration with the private providers, the TurboTaxes—I agree with the panel's comments that this is not just a TurboTax problem, this is not something that can be simply solved by governmental entities. We need the private sector, which has a very vibrant business, as all.

Why have we not created a single easy-to-use portal so that, for Mrs. Smith or the lady from the story in Utah, there is a single place where you can at least check whether this is a real claim or not? I mean, do you all want to speak to that notion of how we do a better job of consumer education and why we have not had the IRS more active in having, perhaps in collaboration with State tax departments and others, an easy-to-find site? And frankly, what would be the responsibility as well of the private-sector providers, the TurboTaxes and others, to collaborate with that one single portal?

Mr. VALENTINE. With the remaining time left, there are two issues that you are really raising. One is the notification issue, and the second one is, how does the taxpayer easily check to see if their return has been filed? Utah actually tried to address both of those issues by having a real-time notification that we believe your return has been hacked or that your return has been filed. We actually tell them.

Senator WARNER. Unlike the IRS.

Mr. VALENTINE. We do not have the impediments that the IRS has in that regard.

The second one is that we have an easy system now for taxpayers to check whether a return has been filed or not. We call it our Taxpayer Access Point or TAP system. You go to our Tax Commission website and you fill out the authentication issues.

Once you have done that, you can determine whether your return has been filed. So we have been doing public service announcements saying, please check to see if your return has been filed. If your return has been filed and you have not filed it, here is the number to call.

Senator WARNER. Well, would it not be potentially better to have some national education process here since, again, the disproportionate amount of the fraud is taking place at the Federal level rather than the State level?

Mr. VALENTINE. I would agree.

Senator WARNER. Commissioner, do you want to——

Commissioner ALLEY. Yes, I would agree as well. It is just a matter of finding the resources and the funding and getting all the players collaborating with one another at the same time. But I think it represents an ideal scenario that should be played out, and we need to strive toward that. We just have to get it started, and we have to have the leadership.

Senator WARNER. I know my time is up, Mr. Chairman, but I would simply say that when we are looking at $5.8 billion in fraud—the *Washington Post* says this year we have seen a 37-fold, 37 times increase in potentially fraudulent claims—the ability to have a little bit of resources to have that common site, number one, and two, either by administrative change or legislative change, making sure the IRS actually informs people when they know they have been the victim of identity theft, I think would be steps in the right direction.

Thank you.

The CHAIRMAN. Well, thank you so much, Senator.

I might add that Senator Grassley is chairman of the Judiciary Committee, and he asked that I ask this question of you, Mr. Camus, and then we will turn to one of the other Senators.

On behalf of Senator Grassley, the Treasury Inspector General for Tax Administration, or TIGTA, has detailed how IRS needs to do more to reduce improper payments for the Earned Income Tax Credit and the Child Tax Credit. For 2013, about $14.5 billion in improper EITC payments were made, and between $5.9 billion and $7.1 billion for the Child Tax Credit.

Now, both of these credits pay cash benefits for exceeding any tax paid, making them a prime target for anyone looking to engage in tax scams or ID fraud. At the same time, the rules governing both these credits are complex, opening them to innocent human error.

So the question is this, Mr. Camus. In your opinion, what amount of improper payments would you attribute to fraud versus innocent taxpayer error, and do you suspect that at least a significant amount of improper payments are the result of fraud?

Mr. CAMUS. Well, it is clear that the fraudsters, as we pointed out today, look for any opportunity whatsoever to get at money, and they are ruthless in their attempts. The fact that they would use credits that are legally available to folks filing tax returns is not a foreign concept. I just do not have that information available, but I would be happy to meet with my audit staff and try to get a response to Senator Grassley.

The CHAIRMAN. If you would, I would like to have that response as well.

Mr. CAMUS. Yes, sir.

The CHAIRMAN. Well, thank you.

Senator Isakson?

Senator ISAKSON. Thank you, Mr. Chairman, Ranking Member Wyden. I appreciate the opportunity.

Ms. Klem, last week I returned home to Atlanta from a week in Washington, and when I walked in the back door, my wife—whose name, by the way, is Diane—said, "You need to listen to the voice mail I saved from the telephone this week."

It was precisely the call you talked about, where a woman with a very convincing voice informed me that the IRS had determined I owed them a substantial amount of money and that I should call a 202 number as quickly as I could or they would file suit next week. Fortunately, being a member of this committee, I realized that probably was not true. But the next morning, ironically, I was

doing a free-file event with the director of the IRS in the Atlanta region and gave him the telephone number to follow up on.

When I gave him that number, he said, "Well, this cannot be real, because we do not make any solicitation by telephone; every one is in the mail." I thought to myself, "I should know that," but the American public ought to know that as well.

So it would seem like there would be more ombudsmanship on behalf of the IRS, and maybe even the IG or the Treasury, to let taxpayers know that there are no enforcements by phone, they are all done by mail, because that is a real problem, and it was a very convincing phone call.

Ms. KLEM. Yes. Thank you, Senator. It is very common, and it is very upsetting when that call comes in. That is precisely why this scam is so successful. We do have partnerships on a local level with our counterparts at FTC, the IRS, and others, and we do share information like this infographic that is in front of me right now, which is a really great infographic—I am happy to share it with the committee—about the IRS imposter scam.

It says: "Warning Signs: How Will the IRS First Contact You? By Phone? No. Email? No. By Mail? Yes." It is very clear to see, but this is not widely disseminated, and so we need to do a better job of getting that into the hands of the general public.

Senator ISAKSON. That is the point I wanted to make. If the chairman would listen, or Ron Wyden would listen for a second, I want to make a point. One of our problems is, we do not have a game plan or a point man to get the consumer information out there, and that has been said by a number of you. We have a department that was created by the administration called the Consumer Finance Protection Bureau, which is in the business of protecting consumers.

It would seem like Secretary of Treasury Lew would contact Richard Cordray and this would be a perfect way for them to use their investigatory and solicitation arm that tries to help people who are victims of business fraud, to protect them from tax fraud as well. I think that is something that Treasury could do.

Mr. CAMUS. Yes, sir, Mr. Isakson. As a matter of fact, we have touched base with the Consumer Finance Protection Bureau, so we are going to include them. The majority of our focus has really been with the Federal Trade Commission and the IRS. The IRS has been putting out YouTube videos, and I myself have been interviewed.

I will take any television interview that is put in front of me, not because I am a ham, but because I believe in my heart that if we protect one taxpayer from having these horrific stories, that is a good day for us. I am so happy about this hearing because I am hoping that this will also help get the word out that when you get those calls, please hang up the telephone. But I really, really appreciate it, and we are trying to work with that bureau.

Senator ISAKSON. And I hope Director Cordray will be as aggressive on protecting people from tax fraud as he is from other frauds in society.

Ms. Ciraolo, I represent Georgia, where Ft. Benning is located. I noticed in your testimony that a member of the medical team at Ft. Benning stole the information and identification of a number of

soldiers at Ft. Benning, and tax fraud was perpetrated against them.

Did you coordinate with the Department of Defense once that was determined to try to get the word out to DoD that they need to watch out for those who would take advantage of their position with the government to steal the identity of our soldiers?

Ms. CIRAOLO. Senator Isakson, thank you for that question. I joined the Department 2 months ago, so I was not involved in those types of discussions. I do not have that information with me today, but I can certainly report back on what efforts were made with the Department of Defense. We certainly take seriously any allegations and efforts by offenders to commit these offenses, and we are particularly focused on the vulnerable victims of our society, including our military members.

Senator ISAKSON. Well, as chairman of the Veterans' Affairs Committee, I am going to take the initiative to do the same thing too, so, if you would do that with DoD leadership, I will do it with Veterans' Affairs leadership as well.

Ms. CIRAOLO. Of course.

Senator ISAKSON. My last point is this. Each of the State Directors made a comment about information sharing, if I am not mistaken, and that would be a key to stopping this. One of the problems that exist is the U.S. Senate and House have not done a cyber-security bill, and, in the pending bill that we hope will be before us soon, there are provisions for idea sharing and exemptions from the anti-trust laws, so information can flow to the government to enforce against tax fraud and things of that nature that are used by cyber-security.

So I would hope we will get the message that we are part of the problem. Our cyber-laws are way out of date with our cyber-criminals, and the quicker we in Congress act on that legislation, the more taxpayers will be safe from fraud. That is my only editorial comment.

The CHAIRMAN. Well, thank you, Senator.

Senator Casey, you are next.

Senator CASEY. Mr. Chairman, thanks very much. I appreciate the hearing and want to thank the witnesses for your testimony, your presence, and your commitment to stopping this crime.

I am struck by what I have seen in Pennsylvania. I am sure this could be replicated in many States, but I am just looking at a small sampling of headlines. This is from a television station in Erie, way up in the northwest corner of our State. The title of the news article about which they were reporting was, "IRS Phone Scams Ramp Up in Erie." Then we go to the other end of the State, literally, the Lehigh Valley over by the eastern border of our State: "IRS Scam, Widespread in Pennsylvania, Reported in Lehigh Valley." Then, in my home area of northeastern Pennsylvania: "IRS Phone Scam Reaching More in Northeastern Pennsylvania." So this is, again, a lot of what you have heard and a lot of what you have had direct experience with trying to stop.

I would start with Assistant Attorney General Ciraolo. I have a particular question about your assessment of kind of where we are in light of what I have seen, and what I am sure others have seen. I was in Berks County, which is on the eastern side of our State,

a number of months ago with the District Attorney, John Adams. Mr. Adams was kind of walking through some of the basic challenges from a prosecutorial standpoint.

He emphasized, among other things, that the perpetrators are, first, highly organized, and two, often reside in jurisdictions far away from the victims, and also beyond the reach of local authorities. And he even pointed to, as you have all seen, I am sure, perpetrators residing in foreign countries. So those are among the many challenges that much of your testimonies pointed to.

I do not want to be pessimistic, because I do want to get to the part of your testimony where you talk about what has been happening with the Justice Department and some of the success you have had, but there is, I think, a sense, because of the scope and gravity of the problem, that we are not winning. I want to just, from a national perspective, ask you, how would you assess the war or the battle?

Ms. CIRAOLO. Thank you, Senator Casey. The Tax Division has a dual role in these matters. We prosecute the offenders, and, in doing so, we hope to change the calculus for would-be offenders with the substantial sentences that we are receiving, and we are receiving substantial and increasing sentences.

In addition, we share information we obtain from these cases in real time with the IRS which, it is our understanding, is working very hard to improve its filters to better identify fraudulent returns and to prevent the issuance of fraudulent refunds. So that is the Tax Division's role. These cases certainly present unique challenges, and we will continue to devote our available resources in this area.

Senator CASEY. And I guess I would ask, starting with you and going down with your colleague from Treasury and others, and I know much of what you might say in the short answer—and it has to be short because of the time—is already imbedded in your testimony. But if you had to itemize one, two, or three action items that we could work on, resources or other tools that you need to do your job—and I am sure others who may not be in the Federal Government but play a role in this—what do you hope we would do by way of authority or authorization or by way of appropriation?

Ms. CIRAOLO. Senator, I think that holding hearings like we are having today is critical to getting the word out to the American public—our elected representatives taking the message back to their home States and making sure the information is out there as often and as loudly as possible.

Many of these scams can be stopped if the American public is educated, and having a centralized location for that information, I think, is a wonderful idea. I am very happy to see the representatives here on the panel from across the country. It gives me hope that we will see further information in the future.

Senator CASEY. Thank you. I would maybe ask each of the remaining witnesses to do a 15-second, "What should Congress do?"

Mr. CAMUS. I echo what my colleague said. From a standard law-enforcement point of view, the scam is so simple. We will never be able to prevent somebody from picking up the phone claiming to be another person and demanding money. It is public awareness at the top of it. When the money dries up, the criminals will go away.

But getting our hands on them, and bringing them to justice in the historic way, is one of the things we want to do because we want people to pay for this, but it is not a solution to the crime. It is people hanging up the telephone and not being victimized.

Commissioner ALLEY. The criminals are going to continue to be very agile, so, as we close one hole, they will open a new one. But I think the greatest thing we can do is to ensure and require greater collaboration among all the groups, as well as provide some funding to ensure that that collaboration can take place.

Senator CASEY. Commissioner, thank you.

Mr. VALENTINE. A final comment is that you still have to be able to cut off the vector that is used to be able to receive the money, and I think the identification of it is something Congress can require the financial industry to do, to say, you know what? We just have to know that this series is going to be a pre-paid debit card. We will not refund it that way, we will refund it by a check at that point.

Senator CASEY. Thank you.

Ms. KLEM. And, Senator, I would echo the comments about education and raising awareness around the issue. I travel the State every day and speak to mostly older adults about this fraud, and it is just devastating to hear their stories. Frequently after they have shared them with me they say, gosh, I wish I had talked to you last week. So, if we can get more awareness, more education, more media spotlight, that would be great.

Senator CASEY. Thank you very much.

Thank you, Mr. Chairman.

The CHAIRMAN. Well, thank you.

Senator Cantwell, you are next.

Senator CANTWELL. Thank you, Mr. Chairman. I would like to join my colleagues who have been bringing up these issues about identity theft and fraud, but specifically to point out that the 111th Congress increased the IRS's responsibility while decreasing the funding, so the IRS is now responsible for implementing the Foreign Account Tax Compliance Act, and the program is in effect for calendar year 2015.

So, in addition to the additional required legal tasks lawmakers will have, the IRS is being urged here—which we really want you to do to combat identity theft—to reduce errors in Federal tax programs and generally reduce tax fraud. So I just think we need to take this into consideration as it relates to the budget this year and make sure that the resources are there to do this.

I am concerned that taxpayers will ultimately—we need to get a handle on what has been happening with identity theft. It was found that the IRS closed 22 percent of the identity theft cases without taking the appropriate steps to fully resolve the victim's account.

So, examples include victims not receiving refunds, or IRS failing to update the victim's address so they could receive an Identity Protection Personal Identification Number. During fiscal year 2014, nearly 270,000 identity theft returns of this type were closed, so, if that reported rate, 22 percent, is accurate, about 60,000 taxpayers were burdened by having their cases closed in a premature fashion.

So what do we need to do to fix that?

Mr. CAMUS. That is a job that would fit in our audit staff's portfolio. When they look and see how the IRS is doing with their identity theft program, one of the things I always look at is the victim interface and how the IRS is processing the claims and the correspondence. I know that the auditors are doing work in that area as we speak.

Senator CANTWELL. But will we have this resolved for this tax season so we are not prematurely closing cases?

Mr. CAMUS. Unfortunately, it is always in hindsight, in the rear view mirror that the audit team looks at the work that was done in a particular filing year, because they need to wait until the cases are closed before they can look back and see how they were handled. So I will share the sentiment.

Senator CANTWELL. Anybody else? Do you, Mr. Alley, or does anybody else have any thoughts about this? I mean, we need to do something better than to have these taxpayers affected this way.

Commissioner ALLEY. I agree. I mean, it creates a tremendous amount of anxiety among the taxpayers. I mean, we also have Taxpayer Administration Services to work with our taxpayers who have been compromised with their identities to ensure that they receive the comfort and knowledge that their return has been properly reflected in their account and properly accounted for. We need to do the same thing at all levels.

Senator CANTWELL. Well, Mr. Chairman, I know that practically every committee has been asked to address the ideas of cybersecurity and move forward, and I think our committee should certainly look at this particular aspect of making sure that our tax filers are also secure as well. So, thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Cantwell.

Senator Wyden has another question.

Senator WYDEN. Thank you, Mr. Chairman. I just did not want to wrap up without giving you a chance, Ms. Klem, to talk about seniors, because I think we know how outrageous it is that seniors get ripped off this way. I mean, we have millions of older people in this country who are walking an economic tightrope every single day. They balance their food bill against their fuel bill, their fuel bill against housing costs.

They get ripped off this way, and it is not some abstraction. They really suffer. So, as we wrap up, I just wanted to finish with this. What else do you think this committee can do to help beef up the fight to protect seniors from these kind of rip-offs?

Ms. KLEM. Senator Wyden, that is a great question. It is true that this particular imposter scam disproportionately affects vulnerable adults, especially older adults. They are home during the day; they answer their phones. That is because they grew up in a time where they were taught that it is rude not to answer the phone and listen to the caller on the other end.

So I think some of the suggestions we have heard today are wonderful, but I am going to keep beating the drum of education and awareness. I think that that is really key. I think if we can let people know that this is a notoriously awful scam and that they should be alert to it and it is not rude to hang up the phone, in

this particular case, I think that is a wonderful educational tool for people, especially older adults. It is very tough. I talk to them every day.

It is going to be a struggle, but I think the more information and awareness we can get out there, the better. I always tell people who come to my presentations or call me on the phone to share their stories with one or two other people, because I think that personal story, that personal touch from somebody who maybe got that phone call and almost fell victim or did fall victim, letting others know, is important.

Senator WYDEN. Thanks for the good work you are doing.

Ms. KLEM. Thank you.

Senator WYDEN. Thank you, Mr. Chairman.

The CHAIRMAN. Well, thank you, Senator.

Senator Menendez?

Senator MENENDEZ. Thank you, Mr. Chairman. To all of our witnesses, thank you for your testimony.

As many have noted, identity theft and tax schemes are some of the fastest-growing crimes in the United States. Not only do the victims, who are disproportionately low-income and vulnerable populations, lose millions of dollars to these schemes each year, they are also subject to, as Ms. Ciraolo noted in her testimony, months, if not years, of overwhelming paperwork, credit problems, and inconvenience.

One constituent of mine, whom I will just refer to as Sandra, experienced this nightmare firsthand. She contacted my office in March of 2013 to request help in order to restore her identity, which had been stolen in 2010. She did not receive her tax refunds for 2010, 2011, and 2012 and was getting nowhere with the IRS over fixing this situation.

Finally, after an additional 2 years—2 years—of working with her, the IRS, and the Taxpayer Advocate's Office, we were finally able to resolve the situation earlier this year. So, Mr. Camus, is the IRS doing enough to resolve cases of identity theft in a timely manner? Is the 4- to 5-year waiting period that Sandra experienced acceptable, in your view?

Mr. CAMUS. In my personal view, no, because I am a criminal investigator, and I know how horrific that type of an experience is for an individual. But I can tell you, based on the audit work that I have read done by my agency, that the IRS has made great strides in trying to be better, faster, and more responsive to the victims.

One of the things that they put in place was an identity theft victim PIN that, in the future years when the taxpayer files, they use to help validate their identity. I understand they are not always 100-percent on that either, but my observation from reading the audit reports that the audit staff has done is that they are making great strides and they are endeavoring to improve.

Senator MENENDEZ. What would you say is the status now of somebody who finds themselves in a situation like Sandra? What would they reasonably expect to be the period of time that their issue would be resolved?

Mr. CAMUS. My understanding is that it would be much better than it was in 2010, 2011, and 2012. But whether or not it is up to par——

Senator MENENDEZ. Four to 5 years was her experience, so better is a relative question. What would you say? What is the average: a year, 2 years?

Mr. CAMUS. Yes, sir. I wish I had that information available, but I do not.

Senator MENENDEZ. Well, I would love to get it from the IRS at the end of the day.

Let me ask this. Commissioner Koskinen testified before this committee in February about the issue of unscrupulous tax preparers. In responding to a question I raised, he said, "The IRS is very concerned about unscrupulous taxpayers" and that there is "a percentage who are crooks, and then there are ones who are a major part of the problem of fraud across the board."

Now, I know the IRS tried to regulate paid taxpayers a few years ago and was rebuffed by the D.C. Circuit Court of Appeals, which argued Congress has not explicitly authorized such legislation. I personally find it exceedingly strange and inappropriate that many States require hair barbers to have a license, but someone filing very complicated tax returns does not need a license.

So, Mr. Camus, how critical is it for the IRS to be able to regulate tax preparers, and would doing so reduce the amount of fraud and identity theft?

Mr. CAMUS. I think it is critically important for anybody who does such an important job in such an important area as tax administration, that there is training available and they are held accountable and there are standards that have to be met.

I know we work closely with our partners in IRS Criminal Investigation and the Department of Justice Tax Division, when we come across an unscrupulous tax preparer, to bring them to justice. I think it is critically important that those individuals whom elderly folks and other people trust and depend on to file very complicated forms—because they do not understand—do not become victimized by the very people whom they trust.

Senator MENENDEZ. Well, let me ask you this. Can you or Ms. Ciraolo quantify for me in any way how much fraud is related to unscrupulous tax preparers?

Ms. CIRAOLO. Senator, we share your concerns with respect to fraudulent tax preparers and believe that the U.S. taxpayers who engage a preparer should be able to trust that person to be competent and qualified to prepare the returns and to prepare an honest and accurate return. In the last year alone, the Tax Division has obtained injunctions against more than 40 fraudulent preparers and promoters and will continue to prosecute those individuals who willfully assist in the preparation of fraudulent returns.

Senator MENENDEZ. So do you have any idea how many tax preparers—this is my final question, Mr. Chairman—how many tax preparers there are?

Ms. CIRAOLO. Senator, I do not have that information in front of me today.

Senator MENENDEZ. Is that number based on complaints, or is it based on the 40 that you—it sounds like a small number compared

to the universe of preparers that I would assume are out there. So is that based on complaints, or is that based on the Service's own investigations?

Ms. CIRAOLO. The Tax Division works with the Internal Revenue Service in identifying fraudulent preparers, and, based on the evidence that we have received, we follow that evidence where it leads and pursue injunctions, where appropriate, against preparers.

Senator MENENDEZ. Do you have a number of complaints filed with you?

Ms. CIRAOLO. I can tell you that, since 2000, we have filed over 500 injunctions against fraudulent preparers.

Senator MENENDEZ. All right. Thank you, Mr. Chairman.

The CHAIRMAN. Well, thank you, Senator.

I want to thank all our witnesses for appearing here today. I also want to thank all the Senators who participated. I think this has been a very good hearing, and hopefully we can move on from here.

Any questions for the record should be submitted no later than Thursday, March 19th. This hearing will be adjourned at this point. Thanks so much. Thanks to all of you. We really appreciate it.

[Whereupon, at 11:30 a.m., the hearing was concluded.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

PREPARED STATEMENT OF HON. MIKE ALLEY, COMMISSIONER, INDIANA DEPARTMENT OF REVENUE

INTRODUCTION

Chairman Hatch, Ranking Member Wyden, and committee members, thank you for inviting me to discuss this important topic with you today. Senator Coats, thank you for that kind introduction. On behalf of Governor Mike Pence and the citizens of Indiana, it is my honor to appear before you today to address this critical issue that faces everyone in the tax and revenue processing industry.

You have asked me to discuss *Tax Schemes and Scams During the 2015 Filing Season.* Specifically, I would like to illuminate the identity theft and tax refund fraud experiences of Indiana over the last two years and note the extent of this challenge facing all government entities in today's environment. And I can tell you from first-hand experience that this is a problem that must be addressed at multiple levels. This morning I would like to address this issue from three perspectives:

First: The nature of the problem and its overall breadth.

Second: Steps Indiana has taken in an effort to combat the problem and lessons we have learned.

Third: Recommendations from our perspective on additional approaches we must take to more fully and effectively address this epidemic issue nationwide.

THE NATURE OF THE PROBLEM

Tax refund fraud is one of several lucrative platforms for criminals to monetize the value of stolen identity information. It is being perpetrated by thousands of culprits from the small time individual fraudster to large, sophisticated criminal enterprises. In the past, it has been very easy with negligible risk of apprehension or prosecution. The advent of electronic filing and processing has enhanced the ability of criminals to utilize economies of scale in filing large volumes of fraudulent returns, at a nominal cost, replicating numerous returns with only minor changes in original identity information. The zeal of departments of revenue to speed up the processing of returns and reducing turn-around time for refunds—all in the spirit of good customer service—also has contributed to the problem making it easier for criminals to take advantage of the system. Our systems were designed to process rapidly and efficiently—not to screen for fraud and fabricated identities.

The Identity Theft Resource Center,[1] in their 2014 Annual Report, created a diagram that effectively illustrates the interrelationship of the criminal activity and our oftentimes disjointed responses. We must develop a coordinated effort to battle ID theft and mitigate the risks of misuse.

---

[1] *http://www.idtheftcenter.org/images/page-docs/2014AnnualReport20150227.pdf.*

In calendar year 2014, twelve percent of the total tax refund dollars requested from Indiana was found to be fraudulent. We identified more than 78,000 fraudulent tax returns filed using manufactured or stolen identities, and prevented more than $88 million in fraudulent refunds from being issued. This mirrors similar statistical reports from the U.S. Government Accountability Office that reports the IRS lost an estimated $5.8 billion to fraudulent refund claims in 2013 while blocking about $24 billion in attempts. They further reported that suspected identity theft incidents for 2013 were nearly 2 million, an increase of more than 350% from 2010. We hear anecdotally from other states that they also are experiencing comparable fraudulent activity.

Though early in the 2015 filing season, we are already seeing a dramatic increase in the use of valid identities which have been stolen. With the advent of reported successful hacks at many large U.S. companies, we believe the availability of valid stolen identities for tax fraudsters has never been greater. This is particularly concerning because stopping fraud with valid identity information is much more difficult than screening for manufactured identities which was the most common practice of fraudsters in the past. The fraudsters have upped their game and we must respond accordingly.

WHAT ARE WE DOING IN INDIANA?

In Indiana, we knew we were suffering some tax fraud based on identity theft, but we did not have a reliable method to calculate the actual impact. In 2012, we began conducting research and analysis of our processes and statistical filing results. We noted that it appeared Indiana was processing more returns and paying out more money in tax refunds than seemed reasonable based on our estimated population growth. Figure 1 (Return Growth) illustrates the growth of our total returns (Red Line) compared to our total refund returns (Blue Line). The green bars show our overall electronic filing percentage. The growth of two hundred thousand taxpayers in a just a couple of years strained credibility, so we looked for other reasons why we would be getting so many more tax returns.

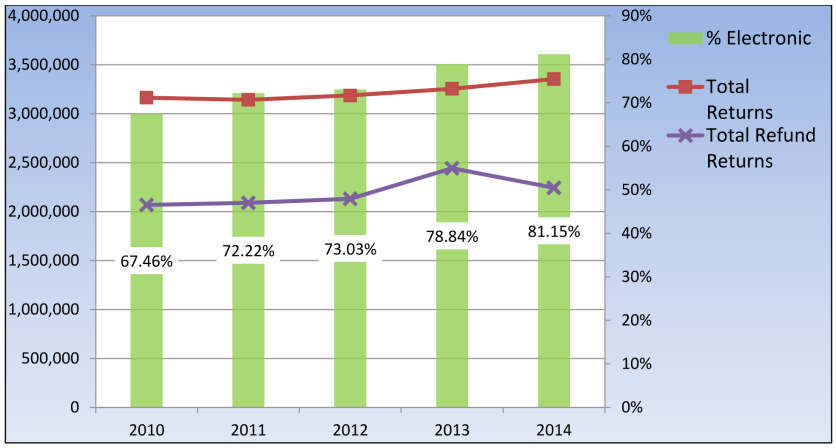

Figure 1: Return Growth

Our analysis determined that identity theft and refund fraud was the most likely explanation for the accelerated growth in returns and refund requests. Once we identified these phenomena, we brought key staff together and worked with the office of Governor Pence and our General Assembly to develop a strategy to define elements of an effective identity fraud program for the Indiana Department of Revenue.

Key objectives of our approach were:

1. Ensure that we do not mistreat legitimate taxpayers because of a small number of dishonest individuals.
2. Protect taxpayer dollars *and* taxpayer identities.
3. Protect state revenues from issuance of fraudulent refunds.
4. Identify the criminals for deterrence efforts.
5. Ensure fraudulent dollars do not affect our revenue based distributions and financial reporting.

These became the guidelines that our identity protection team would follow. We knew that we needed to make significant systemic modifications and we needed to do it before the next tax season. Staff reached out to our fellow states through the Federation of Tax Administrators (FTA) and our partners at the IRS to see if there were ideas that we could borrow and implement.

The response was very supportive and we were welcomed to view, visit, and exchange ideas with our counterparts across the United States. Many of them had partial solutions or had tried to implement incremental improvements. The time we spent working with other states confirmed that Indiana was less prepared and needed to catch up. On the positive side, we discovered that there were ready-made commercial solutions that we could bring to Indiana that could have a major impact in a short period of time.

Governor Pence reviewed the data we provided and the potential solutions the department suggested. With his support, we initiated a pilot program to screen all returns for suspicious identities. The program used LexisNexis, a third party commercial vendor, to screen the returns and note identity information such as name, address, social security number, or other identifier information that appeared suspicious. Processing of those returns screened as suspicious was suspended and an identity confirmation quiz request was sent to the taxpayer at their filing address. Taxpayers were asked to confirm their identities by completing a short quiz. They could log into a secure website or could call our call center where we had dedicated analysts to handle their quiz. As a result of implementing this pilot effort the department expected to directly reduce fraudulent refunds by $25 million with an investment of $8 million in staffing and technology. Our actual results confirmed more than $88 million of attempted refund fraud identified and stopped with $42 million attributable directly to this identity screening tool.

The identity confirmation quiz is very powerful and made a significant difference. But it is not a panacea. It is only part of a larger process to strategically focus on identity theft and refund fraud which encompassed additional talent, new procedures, and new IT systems. We made it clear in the beginning that the department would need to make systematic changes. We took the following steps:

1. Procured an identity confirmation vendor (LexisNexis)
2. Hired additional staff
3. Conducted a public relations campaign
4. Made agreements with software vendors to begin setting standards
5. Began modernizing infrastructure to specifically confirm identity information and recognize fraud trends

Figure 2 (2014 Indiana Fraud by Source) demonstrates that we stopped more than $88 million in fraudulent refunds being paid to manufactured or stolen identities in the pilot year alone (2014). The identity screening via the identity confirmation quiz was the simplest fraud to stop and we took advantage of that simple process to concentrate on the more sophisticated fraud schemes using our enhanced professional analysts and early analytics.

Source	# of Returns	Description	Total Refunds Stopped
Analyst Review	34,300	Investigation and decision by trained fraud prevention staff	$45,642,625
Identity Confirmation Quiz	43,918	No response to Identity Confirmation Quiz notifications	$42,426,289
Calendar Year 2014 Total			**$88,068,914**

Figure 2: Indiana 2014 Fraud by Source

In one sense, the $88 million was gratifying—but it was also astonishing. The problem was much larger than we had anticipated. The end-of-year fraud statistics were interesting as well. Almost four percent of returns we processed in 2014 were identity fraud. A surprising data point was that these 78,000 returns represented 12% of the value of all refund requests. While this was higher than expected, it makes sense when we consider that the fraudsters are attempting to maximize their profitability. We also identified that Indiana paid out $4 million in identity fraud refunds that we later identified as fraudulent but were unable to stop. Some fraud gets through before we can identify a new pattern and react. This illustrates that our efforts to identify and stop refund fraud must continue.

We could not have achieved these positive results without additional resources and multiple components to our identity theft and refund fraud program, including an $8 million augmentation to the department's budget. Indiana added 15 call center people to assist our taxpayers with the identity confirmation quiz. We also added eight additional fraud analyst positions, a prosecutor with fraud experience, a public relations professional, and information technology professionals.

Our public relations campaign was critical to our success in educating citizens, rallying market professionals, and explaining the outcomes to stakeholders and media. This allowed us to alert our taxpayers that protecting their identities was

a priority for us and though it might slow down the refund process slightly, it would better ensure protection of their identities and avoid a strain on state finances. Further, it provided assurance that if they should receive an identity confirmation quiz, it was legitimate and no cause for alarm.

One quiet, but crucial, key to our success was gaining more control of the interfaces and behavior of our software vendor partners. During the 2014 filing season, we began tracking fraudulent returns submitted by each software vendor. As the Fraud by Software Vendor Table (Figure 3) clearly demonstrates, there was a large variability among software vendors of the incidence of fraud. The data shows that some vendors are taking fraud seriously and implementing protective screening while some are either unaware of, or unable to stop fraud. A few vendors claimed that they were not responsible for doing any fraud prevention at all.

	Fraud by Refund Return Count (%)	Fraud by requested refund amount (%)
Highest	92%	85.0%
Average	22.3%	11.0%
Median	6%	2%
Mode	1%	1%
Lowest	1%	0%

Figure 3: Fraud by Software Vendor

As a result, in 2015 Indiana required that all software vendors wishing to be certified to file Indiana returns sign agreements with the state. The agreements made it clear to vendors that they would be monitored for the fraud they sent along to Indiana. Software vendors that experienced excessive fraud in 2014 were not certified unless they provided evidence of increased fraud screening on their part. We concluded that there is no reason to maintain a business relationship with a vendor that is not playing their part in fraud prevention.

For the 2015 filing season, we have continued to make significant enhancements to our identity theft and refund fraud program. We continue to use the identity theft screening tool contracted with LexisNexis with enhanced elements based upon lessons learned. In addition, we have implemented a new pre-filter processing platform that provides us the ability to run all of our individual returns through an extensive screening prior to being processed in our normal returns processing system. This pre-filter process includes a decision matrix toolset which allows us to establish multiple filter parameters to detect fraudulent returns and unusual activity. This provides dramatically enhanced agility and adaptability during the filing season as we experience various patterns or learn of new issues so that processing rules and parameters can be easily adjusted. This pre-filter platform was built with the assistance of Revenue Solutions, Inc. (RSI), a third party vendor specializing in tax processing.

LESSONS LEARNED

We are still early in battling this problem but the following early lessons are apparent:

1. Strategic priority: identity theft and refund fraud have escalated dramatically over the last two years and in order to effectively combat the problem, it must be a strategic priority. This demands making a fiscal investment in leadership, staff, technology, and third party resources. Priority support must be in place from the top down. Governor Pence has consistently supported our efforts to combat identity theft and refund fraud, which has been crucial in our ability to continue to invest in and improve our program.
2. Collaboration: no one has all of the answers. The perpetrators are sophisticated and agile, moving from one vulnerability to the next. Sharing data, best practices, and experiences among revenue agencies, both state and federal, along with software vendors and support vendors is critical. The Federation of Tax Administrators (FTA) has actively assumed a key role as facilitator but must be strongly supported by all parties involved.

3. Taxpayer Support: Taxpayers are willing to be part of the solution if they understand what you're trying to achieve. We received minimal resistance to the identity confirmation quiz. However, communicating in advance that this is a valid tool and not another scam is critical.
4. Targeted Solutions: There are many types of fraud, fraudsters, and different means for filing returns. It is important to understand the intricacies so that targeted solutions can be developed and applied. We can no longer review returns individually but must identify broad traits so that we can systemically identify suspicious activity and address it collectively. In the past, we treated all fraud the same which is neither efficient nor necessary.
5. Prepaid Debit Cards: Use of prepaid debit cards is the preferred tool of fraudsters in receiving their refunds. They can be purchased with virtually no identification or registration and are readily transferable from the card to gift cards, bank accounts, other debit cards, or even to purchase goods and services.
6. Fraudsters Hide: Sophisticated fraudsters use stolen or invalid identities to open bank accounts, transfer money, and further insulate themselves from the refund once it is received. This makes it even more difficult to apprehend and prosecute the culprits.
7. Manufactured Identity: A "Manufactured Identity" is one where the fraudsters have simply filled out federal or state returns with completely made up identities and tax data. They may use celebrity names or obscure names with bogus addresses and social security numbers and have the refund deposited to a prepaid debit card that requires virtually no purchaser identification. These are often being perpetrated by relatively unsophisticated fraudsters and rely upon tax software vendors that allow filing fees to be deducted from the refund itself thus requiring no cash outlay in advance. Fortunately, our LexisNexis identity confirmation tool is very effective at identifying these fraudulent attempts as the identity information does not match to valid external information.
8. Unlinked Return: An "Unlinked Return" is one that does not have a federal tax return associated with it and is filed directly with a state bypassing many of the IRS fraud safeguards. This unlinked return process is also used by fraudsters to file in multiple states rather than simply one using the same fraudulent identity. Though it is possible to have a valid unlinked return, the rate of fraud is very high and requires additional review.
9. Synthetic Identity: A "Synthetic Identity" is one which has been amalgamated from existing identity information such as children or deceased relatives and contains enough valid identity information to appear to be a valid identity.
10. Stolen Identity: A "Stolen Identity" is one where the fraudsters have obtained valid taxpayer information comprised of names, addresses, social security numbers, and sometimes even dependents, from real taxpayers. These culprits then seek to gain fraudulent refunds in two ways. First, they file a federal return early in the filing season before the real taxpayer submits their valid return. Second, they file directly with a state, or multiple states, that is usually not where the valid taxpayer is actually located.

THE ULTIMATE APPROACH TO COMBAT THIS PROBLEM

In order to effectively overcome the problem of identity theft and refund fraud, all parties involved must work collaboratively. We must develop cross-functional teams with significant coordination among the three key players in our tax system. Consider the Three Legged Stool concept depicted in Figure 4 which notes that the states, the IRS, and software vendors each represent an important leg of the stool. Each has unique data, perspectives, and capabilities that the system as a whole requires in order to make better decisions.

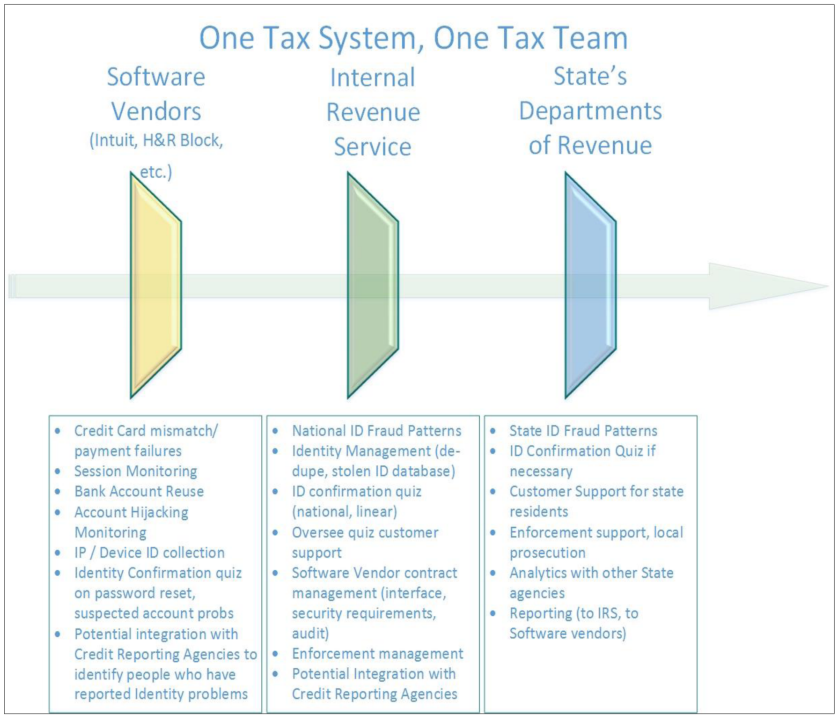

Figure 4: Three Legged Stool

The "three legged stool" concept allows each leg to execute appropriate roles within our present tax system resulting in an effective and collective solution.

Indiana believes that our partners at the IRS are in the best position to centrally manage the highly sophisticated fraud. The IRS can help the states define the expected behavior of the software vendors which could include security requirements, potential fraud reporting, and corrective behavior for vendorsnot operating according to the systematic norm. The central location in this process also makes the IRS a better place to accomplish analytics to identify multi-state fraud patterns, manage a shared database, correlate with other data sets (Social Security Administration and others), and coordinate national and international enforcement efforts. Without data driven prosecution and enforcement, the culprits face little risk in continuing to conduct this sort of activity.

States must also work collaboratively with one another to develop and share effective analytics, algorithms, and best practices. The Federation of Tax Administrators (FTA) has convened a Fraud Working Group comprised of multiple states, including Indiana, that have already made a significant commitment to developing taxpayer identification validation standards and consistent communication and monitoring mechanisms to ensure that uniform data elements can be captured and shared. Their intent is to establish uniform practical measures that the software vendor industry can support and that will be applied consistently, avoiding disparate rule sets and expectations from each state. This will enhance the likelihood of industry compliance. The FTA has also positioned itself as a facilitator and clearinghouse for the states as well as the IRS in sharing best practices and innovations. They can be very effective in helping communicate with members the importance of identity theft and refund fraud prevention programs and the positive economic impact it will have. States must recognize this value and be willing to commit the necessary resources.

Software vendors must be responsive to the IRS and states as they learn more about the methods used by fraudsters. We have already learned that account access must be protected with multi-factor authentication. However, software vendors also have multiple other data sources and analytics which they must be willing to use to stop fraud from inception. Further, as their intelligence increases, they must be willing to share that intelligence with states and the IRS as their partners.

CONCLUSION

In conclusion, I would like to emphasize the following points:

First, identity theft and refund fraud is an epidemic problem and growing rapidly. It currently represents one of the easiest means available for fraudsters to monetize stolen identity information. We are all aware of the increased vulnerability we face for protection of identity information.

Second, collaboration and information sharing among the IRS, state departments of revenue, and tax processing and software vendors is essential. Strengthening of the "three legged stool" by tax processing partners will allow us to more effectively combat identity theft and refund fraud through enhanced analytics, sharing of information, and implementation of best practices. This sharing and collaboration must be in real time, not days or weeks down the road. Delays in digesting new information or implementing good ideas leaves the window of vulnerability open longer for fraudsters to enter.

Third, investment in identity theft and refund fraud prevention tools will provide a strong return on investment. In 2014, Indiana realized greater than a 10 times return on investment based upon fraudulent refunds stopped compared to actual program costs. I encourage states as well as the federal government to make our battle against identity theft and refund fraud a strategic priority. This also means backing that priority with necessary funding to move the dial. I'm confident it will provide a significant return on investment and also protect our citizens.

On behalf of Governor Mike Pence and the citizens of Indiana, I thank you for your time today. I appreciate the committee's willingness to examine this issue and we in Indiana stand ready to assist and participate in a comprehensive solution.

PREPARED STATEMENT OF TIMOTHY P. CAMUS, DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS, TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, DEPARTMENT OF THE TREASURY

Chairman Hatch, Ranking Member Wyden, and Members of the Committee, thank you for the opportunity to testify on the topic of Tax Schemes and Scams during the 2015 filing season.

I also want to thank you for holding a hearing on this topic, for by doing so, you are bringing attention to these schemes and scams, and thereby alerting your constituents and others across the country to their existence. By raising public awareness about such efforts to swindle people out of their money, we may prevent the next person from becoming a victim. And if we protect even one taxpayer from this type of theft, we have done a very good thing.

The Treasury Inspector General for Tax Administration, also known as "TIGTA," is statutorily mandated to provide independent audit and investigative services necessary to protect the integrity of Federal tax administration as well as to improve the economy, efficiency, and effectiveness of Internal Revenue Service (IRS) operations. TIGTA's role is critical in that we provide the American taxpayer with assurance that the approximately 91,000 IRS employees, who collected over $3.1 trillion in tax revenue, processed over 242 million tax returns and other forms, and issued $374 billion in tax refunds during Fiscal Year (FY) 2014, did so with the highest degree of integrity and in an effective and efficient manner while minimizing the risks of waste, fraud, or abuse. This includes investigating individuals who use the IRS as a means of furthering fraudulent, criminal activity that could call into question the integrity of the IRS, as well as investigating allegations of serious misconduct by IRS employees and investigating threats of violence against the IRS, its employees, and facilities. Over the past year, a significant part of our workload has been devoted to investigating scams that can negatively impact the integrity of tax administration.

Tax scams are nothing new. For at least the last decade, the IRS has provided the public with information about what it sees as the "Dirty Dozen" tax scams on

its website. These scams range from offshore tax avoidance to fake charities and inflated refund claims. Compiled annually, the "Dirty Dozen" lists a variety of common scams that taxpayers may encounter. However, many of these scams peak during the filing season as people prepare their returns or utilize the services of paid preparers.

The 2015 filing season has unfortunately brought more of the same. However, there are two tax scams in particular that are among the most pernicious and dangerous. They have proven to be surprisingly effective and fast ways to steal taxpayers' money, and in this fast-paced electronic environment, the money can be gone before the victims ever realize they have been scammed.

PHONE IMPERSONATION SCAM

The phone impersonation scam has proven to be so large that it is one of my agency's top priorities, and it has also landed at the top of the IRS's "Dirty Dozen" tax scams this year. The number of complaints we have received about this scam make it the largest, most pervasive impersonation scam in the history of our agency. It has claimed thousands of victims, including victims in every State represented on this committee, with reported losses totaling more than $15.5 million dollars to date. Here is how it works:

The intended victim receives an unsolicited telephone call from a person claiming to be an IRS agent. The caller, using a fake name, tells the victim their "badge number," and claims that they owe taxes and are criminally liable for an amount owed. The callers may even know the last four digits of the victim's Social Security Number (SSN). They then threaten the victim by stating that if they fail to pay the amount immediately, the victim will be arrested, a suit will be filed, or some other form of adverse official action will be taken. These actions have been reported to include loss of a driver's license, deportation, or loss of a business license. They often leave "urgent" callback requests and call multiple times. Although these callers initially preyed on the most vulnerable people, such as the elderly, newly arrived immigrants and those whose first language is not English, they have expanded their scam to people from every walk of life. The continued number of people receiving these unsolicited calls from individuals who fraudulently claim to represent the IRS is alarming.

We first started seeing concentrated reporting of these calls in August, 2013. As the reporting continued through the fall, in October 2013, we started to specifically track this crime. To date, we have received hundreds of thousands of complaints about these calls. According to the victims, the scam artists made the threatening statements as described above, and then demanded that the victims immediately put money on prepaid debit cards in order to avoid being immediately arrested. The callers often warned the victims that if they hung up, local police would come to their homes to arrest them. The scammer may also send bogus IRS e-mails to support their scam. Those who fell for the scam withdrew thousands of dollars from their bank accounts and then purchased the prepaid debit cards as instructed by the callers. Once the prepaid debit cards were purchased, the criminals instructed the victims to call them back and to read the numbers off of the prepaid card. By the time the victims realized they had been scammed, the criminals had negotiated the prepaid cards and the money was long gone.

One particularly sad story was shared with TIGTA by a member of this Committee in a letter written on behalf of a constituent regarding the tragic death of the constituent's father as a result of receiving several threatening calls from a scammer claiming to be from the IRS and demanding money. This scam has cost thousands of taxpayers millions of dollars, but to my knowledge, this may be the most heartbreaking result. TIGTA continues to work with the IRS to strengthen its efforts to crack down on this type of abuse and try to prevent other vulnerable individuals from being victimized by this kind of fraud.

To date, TIGTA has received over 366,000 reports of these calls. We receive between 9,000 and 12,000 reports of these calls each week. As of March 9, 2015, 3,052 individuals have been victimized by this scam by paying a total of $15.5 million, averaging over $5,000 per victim. The highest reported loss by one individual was over $500,000. In addition, 296 of these victims also provided sensitive identity information to these scammers. The scam has claimed victims in almost every State in the country. For example, taxpayers in Utah have lost more than $276,000 to this scam, and taxpayers in Oregon have lost more than $180,000. As of February 28, 2015, the top five States for total dollar losses by victims are California ($3,840,000),

New York ($1,352,732), Texas ($795,884), Florida ($760,000), and Virginia ($648,363).

The criminals do not discriminate; they are calling people everywhere, of all income levels and backgrounds. In fact, I myself received one of these calls on my home telephone on a Saturday, and you may also have received a call or know of a family member or constituent who has received one as well. Based on reviewing the complaints we have received, we believe the calls are now being placed from more than one source. This scam is the subject of an ongoing multi-agency investigation. For this reason, there is much that we are doing to apprehend the perpetrators, but I am not at liberty to disclose specifically what is being done as it may impede our ability to successfully bring these criminals to justice. I can tell you it is a matter of high priority for law enforcement. As I told the individual who called me on my home phone, "your day will come."

In the meantime, we are investigating some of the individuals who process the money, and most recently we arrested two individuals associated with this type of scam. The two individuals were arrested and prosecuted for their role in converting the prepaid money cards. When interviewed, one of the defendants estimated she had used prepaid debit cards to purchase approximately $5,000 in money orders per day, six days a week, since November 2013, or roughly $900,000 in money order purchases between November 2013 and July 2014.[1] In another case, in March 2014, an individual was indicted for using an impersonation scam. More specifically, he was indicted for extortion, false impersonation, and fraud.[2]

However, there is much more that needs to be done, as these three examples are part of a broader ring of scam artists operating beyond our borders. This is unfortunately similar to most of the cybercrime we are seeing today—it is international in nature and committed using technology, *e.g.,* in the case of the phone fraud scam, the use of Voice over Internet Protocol technology, and much of it originates from a computer outside of the United States. To further deceive their intended victims, by using this technology, the criminals create false telephone numbers that show up on the victim's caller ID system. For example, the criminals make it appear as though the calls are originating from Washington, D.C., or elsewhere in the United States.

I am also concerned that these criminals and their copycats, like the bank robbers of old, will go where the money is, and will keep using this scam as long as people fall victim to it. For example, we have noted an increasing number of recent reports that the calls are coming in using robo-call technology. When the robo-calls are used, the scammers leave messages demanding that the victim immediately call back a telephone number and speak to a representative. Although the robo-calls are a different approach, the outcome is the same: once the criminal gets the victim on the phone, they demand immediate payment and threaten the victim with arrest for failing to comply with their demands.

Accordingly, we are reaching out aggressively by granting media interviews with all the major networks, and issuing warnings and multiple press releases to the media in conjunction with the IRS and the Federal Trade Commission (FTC), as well as providing this testimony to your Committee. Our message is simple: If someone calls unexpectedly claiming to be from the IRS with aggressive threats if you do not pay immediately, it is a scam artist calling. The IRS does not initiate contact with taxpayers by telephone. If you do owe money to the IRS, chances are you have already received some form of a notice or correspondence from the IRS in your mailbox.

To recap, the IRS will never:

- Call to demand immediate payment, nor will the IRS call about taxes owed without first having mailed you a notice;
- Demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe;
- Require you to use a specific payment method for your taxes, such as a prepaid debit card;
- Ask for credit or debit card numbers over the phone; and
- Threaten to bring in local police or other law enforcement groups to have you arrested for not paying.

---

[1] S.D. Fla. Crim. Compl. filed Sept. 5, 2014.
[2] S.D.N.Y. Indict. filed Mar. 6, 2014.

Remember, also, the IRS does not initially use e-mail, text messages, or any social media to discuss your personal tax issue involving taxes owed or refunds. For more information on reporting tax scams, go to *www.irs.gov* and type "scam" in the search box. If you have been targeted by this scam, report the incident to TIGTA at *www.tigta.gov* by clicking on the IRS Impersonation Scam Reporting tab in the upper right corner, or call the TIGTA hotline at 1–800–366–4484. In addition, contact the FTC and use their "FTC Complaint Assistant" at *www.ftc.gov*. Please add "IRS Telephone Scam" to the comments of your complaint. If you know you owe taxes or think you might owe, call the IRS at 1–800–829–1040. They can help you with a payment issue.

LOTTERY WINNINGS

The lottery winnings scam we are seeing this filing season is a continuation of an older scam. It starts with an e-mail or telephone call stating that you have won the lottery and in order to collect the winnings, you need to send money to prepay the tax to the IRS. The lottery scam often, but not always, originates from outside of the United States, and continues because it capitalizes on a very common dream; getting rich quick and hitting the jackpot.

In one of the largest cases of this type, an individual and his co-conspirators operated a scheme to defraud numerous individuals through Internet solicitations, stealing more than $1 million as well as the identities of the victims. The criminals obtained and used massive e-mail distribution lists containing thousands of e-mail addresses to send unsolicited e-mails falsely informing victims that they had won a lottery or had inherited money from a distant relative. Follow-up e-mails instructed the victims to provide personal and bank account information to receive their lottery winnings or inheritance. Subsequent e-mails to victims falsely indicated that a Government or a quasi-governmental agency, such as the IRS or the United Nations, would not pay the money due to them because advance payment of taxes and other fees was required. The e-mails solicited the victims to wire money to pay the taxes and other fees to designated bank accounts controlled by the criminals.[3]

However, if the victims were unable to pay the taxes and fees, the criminals offered to loan them the money. The victims were then convinced to open online bank accounts and provide the necessary login information to the criminals. Using this information, the criminals stole money from various other bank accounts, transferred that stolen money to the victims' accounts, and then instructed the victims to wire the money to foreign bank accounts controlled by the criminals. In the end, the victims never received any lottery winnings, inheritance, or other money in connection with the scheme; however, they may have received much grief for unknowingly being placed in the middle of a money laundering scheme.

The lead defendant was sentenced to a total of 30 months of imprisonment and five years of supervised release for Aggravated Identity Theft and Conspiracy to Commit Wire Fraud. He was also ordered to pay $1,741,822 restitution to his victims and a $200 assessment.[4]

OTHER FRAUDS IMPACTING TAX ADMINISTRATION

IDENTITY THEFT

The IRS continues to make improvements in its identification of identity theft tax returns at the time the returns are processed and before fraudulent tax refunds are released. The IRS has described identity theft as one of its "Dirty Dozen" and recognizes that new identity theft patterns are constantly evolving and, as such, it needs to adapt its detection and prevention processes.

Notwithstanding improvements in its detection efforts, the IRS still does not have timely access to third-party income and withholding information. Most of the third-party income and withholding information is not received by the IRS until well after taxpayers begin filing their tax returns. For example, the deadline for filing most third party information returns with the IRS is March 31, yet taxpayers began filing their tax returns for the 2015 Filing Season on January 20th. As of February 27, 2015, the IRS has received approximately 58.5 million individual tax returns. Legislation would be needed to accelerate the filing of the information returns.

---

[3] E.D.N.Y. Response to Defendant's Sentencing Letter filed Dec. 19, 2011 and E.D.N.Y. Superseding Info. Filed May 10, 2011.

[4] E.D.N.Y. Judgment filed Dec. 27, 2011.

The IRS has taken steps to more effectively prevent the filing of identity theft tax returns by locking the tax accounts of deceased individuals to prevent others from filing a tax return using their name and SSN. The IRS has locked approximately 26.3 million taxpayer accounts between January 2011 and December 31, 2014. These locks prevent fraudulent tax returns from entering the tax processing system. For Processing Year 2014,[5] the IRS rejected 338,807 e-filed tax returns and stopped 15,915 paper-filed tax returns through the use of these locks as of September 30, 2014.

Additionally, the IRS continues to take steps to more effectively detect and prevent the issuance of fraudulent refunds resulting from identity theft tax return filings. The IRS continues to expand identity theft filters to identify fraudulent tax returns at the time they are processed. It has expanded the number of identity theft filters used to identify potentially fraudulent tax returns and prevent the issuance of fraudulent tax refunds from 114 filters during Processing Year 2014 to 196 filters during Processing Year 2015. The identity theft filters incorporate criteria based on characteristics of confirmed identity theft tax returns.

Tax returns identified by these filters are held during processing until the IRS can verify the taxpayer's identity. As of January 31, 2015, just 11 days after the filing season began, the IRS reported that it identified and confirmed 264 fraudulent tax returns and prevented the issuance of more than $2 million in fraudulent tax refunds as a result of the identity theft filters.

In addition to the above actions, the IRS developed and implemented a clustering filter in response to TIGTA's continued identification of large volumes of undetected potentially fraudulent tax returns with tax refunds issued to the same address or deposited into the same bank account. The clustering filter tool groups tax returns based on characteristics that include the address, zip code, and/or bank routing numbers. Using this tool, the IRS reports that as of October 9, 2014, it identified 517,316 tax returns and prevented the issuance of approximately $3.1 billion in fraudulent tax refunds.

PRISONER FRAUD

Refund fraud associated with prisoner SSNs remains a significant problem for tax administration. The number of fraudulent tax returns filed using a prisoner's SSN that were identified by the IRS increased from more than 37,000 tax returns in Calendar Year 2007 to more than 137,000 tax returns in Calendar Year 2012. The refunds claimed on these tax returns increased from $166 million to $1 billion. As of February 28, 2015, the IRS reports that it identified 24,011 potentially fraudulent tax returns filed by prisoners for screening.

In September 2014, TIGTA reported that the IRS has not yet shared fraudulent prisoner tax returns and return information with Federal or State prison officials.[6] As of June 2014, the IRS has yet to complete needed agreements to begin sharing information related to false prisoner tax returns and return information with Federal and State prison officials. This is despite the fact that the IRS was initially given the authority to share certain information with Federal prison officials in October 2008. The authority for the IRS to share information with prison officials is intended to enable prison officials to take action to punish prisoners for perpetrating fraud and to help stop this abuse of our tax system.

TIGTA also found that the required annual prisoner fraud reports to Congress are not timely and that the reports do not address the extent to which prisoners may be filing fraudulent tax returns using a different individual's SSN. In addition, we followed up on a condition identified in a past review and found that IRS processes still do not ensure that all tax returns filed using a prisoner SSN are assigned a prisoner indicator. Our analysis of tax returns filed during Calendar Year 2013 identified 43,030 tax returns that were filed using a prisoner SSN that were not assigned a prisoner indicator. When tax returns filed using a prisoner SSN are not assigned the required indicator, the tax return will not be subjected to the IRS's specialized prisoner fraud checks.

---

[5] A processing year is the calendar year in which tax returns are processed by the Internal Revenue Service.

[6] TIGTA, Ref. No. 2014–40–091, *Prisoner Tax Refund Fraud: Delays Continue in Completing Agreements to Share Information With Prisons and Reports to Congress Are Not Timely or Complete* (Sept. 2014).

UNSCRUPULOUS TAX PREPARERS

Tax preparers who steal a client's identity information or their tax refunds can also cause great harm to the integrity of the Federal tax system. The following case highlights an example of this damage.

Last December, an Ohio accountant was sentenced for wire fraud, engaging in monetary transactions in property derived from specified unlawful activity, mail fraud, and attempting to interfere with administration of the internal revenue laws. The accountant was sentenced to 36 months in prison, followed by three years of supervised release, and was further ordered to pay $987,050.00 in restitution to victims.[7] From approximately 2009 through 2013, the accountant engaged in various schemes to defraud individuals to obtain money and property by means of false and fraudulent pretenses and representations, and to obstruct the due administration of the Internal Revenue laws.[8]

After the IRS issued a levy to a financial firm in the amount of $91,193.53 to collect taxes owed by one of his clients, the accountant transmitted, via e-mail, a falsified IRS Form 668–D, Release of Levy, which purported to remove the levy from the couple's account. The accountant did so knowing the IRS had not authorized the release of the levy from that account.[9]

Prior to this, around April 2011, the accountant devised a scheme to defraud another victim, a senior citizen with little experience managing financial matters. The accountant falsely represented to the victim that the victim owed the IRS a substantial amount of taxes, and directed the victim to send him multiple payments for taxes purportedly owed by the victim. The accountant kept all of the money received from the victim and used it for his own personal and business expenses, defrauding the victim of approximately $237,050.[10]

In a different case, a tax preparer used the means of identification of other people to file false income tax returns and obtain refunds from the IRS. The preparer obtained most of the means of identification from his previous employment as a tax preparer and from other employment positions he held. He provided this information to co-conspirators so they could also file false income tax returns and obtain refunds from the IRS. The preparer and his co-conspirators ultimately defrauded or attempted to defraud the IRS out of at least $560,000 in tax refunds.[11]

PHISHING SCAMS

Phishing is a scam that has been around for several years and is typically carried out through the use of unsolicited e-mails or a fake website that poses as a legitimate site in order to lure potential victims in to either pay some sort of fee, or provide valuable personal and financial information. Armed with this information, a criminal can commit identity theft or financial theft. Phishing is often used as the technique to gather information to start other scams, such as the lottery scam identified earlier.

My investigators are alerted to hundreds of new phishing scams every year. For example, my agents can encounter numerous fake e-mails that lead to fraudulent websites appearing to be legitimate, but actually looking to steal taxpayers' personal information or to trick the victim into paying money. Also by clicking on any of the links in these e-mails or websites, innocent taxpayers have unknowingly invited the criminal into their computer where they can steal financial information, personal contact information, and even file more fraudulent documents. All the while, this activity is unknown to the victim.

The best thing taxpayers can do is to be alert and to stop and think before clicking on any link. The first contact a taxpayer receives from the IRS will not be made via e-mail. If they receive an unsolicited e-mail that appears to be from either the IRS or an organization closely linked to it, they should be leery and call the IRS to verify the contact and report it by sending it to *www.phishing@irs.gov*.

TIGTA and the IRS office of Online Fraud Detection and Prevention work closely together to protect innocent taxpayers from criminals who create fake websites that impersonate the IRS. In fact, since 2012, when the number of identified phishing

[7] E.D. Pa. Judg. filed Dec. 16, 2014.
[8] E.D. Pa. Indict. filed Jan. 9, 2014; E.D. Pa. Info. filed June 3, 2014.
[9] Id.
[10] E.D. Pa. Info. filed June 3, 2014.
[11] S.D. Cal. Superseding Indict. filed June 19, 2012.

sites peaked at almost 19,000, we have seen a reduction in the number of identified phishing sites over the past two years to 1,200 in 2014.

Chairman Hatch, Ranking Member Wyden, thank you for the opportunity to share my views. This concludes my testimony on some of the tax schemes and scams we have noted during the 2015 filing season. Much work is being done on multiple fronts to dismantle many of these schemes and scams, and our hope is that if we return to testify next year, these incidents will be greatly reduced or eliminated.

PREPARED STATEMENT OF CAROLINE CIRAOLO, ACTING ASSISTANT ATTORNEY GENERAL, TAX DIVISION, U.S. DEPARTMENT OF JUSTICE

Chairman Hatch, Ranking Member Wyden, and Members of the Committee, thank you for the opportunity to appear before you this morning to discuss the Department of Justice's efforts to combat tax refund fraud arising from identity theft.

The Department greatly appreciates the commitment that the Chairman, the Members of the Committee, and the staff have made to highlighting and addressing this important issue. Combatting the illegal use of social security numbers and other personal information to file false returns seeking fraudulent refunds is a top priority of both the Tax Division and the United States Attorneys' Offices across the country. Your efforts to bring attention to this growing and insidious crime will help educate taxpayers about the importance of detecting and reporting identity theft and tax fraud. Today's hearing also sends a strong message to those who would commit these crimes that their schemes will be detected and that they will be prosecuted to the fullest extent of the law.

Using a variety of civil and criminal enforcement tools, the Division, with the assistance of our partners at the IRS and in the United States Attorneys' Offices, has successfully enjoined hundreds of unscrupulous return preparers and other individuals who viewed the Federal Treasury as a personal bank account. Their schemes have included filing returns containing inflated, false deductions or false W–2 income statements, or preparing returns and failing to remit the refund to the taxpayer. In recent years, an even more aggressive scheme has spread across the country at an alarming rate—stolen identity refund fraud ("SIRF").

The plan is frighteningly simple—steal social security numbers, file tax returns showing a false refund claim, and then have the refunds electronically deposited or sent to an address where the offender can access the refund checks. In many cases, the taxpayer whose social security number has been compromised will later face difficulties when he or she files a tax return after the IRS received a false return using that taxpayer's social security number. In other cases, the false returns are filed using social security numbers of deceased taxpayers or others from whom no federal tax return may be due for filing. These schemes are usually implemented in early January, before the proper taxpayer is expected to file their returns, with the goal of taking advantage of the IRS's efforts to pay out refunds quickly. In many cases, the most vulnerable in our society are the victims of this form of identity theft. Names and social security numbers have been stolen at medical firms, prisons, and hospitals by dishonest employees who are often paid for the information. Postal workers have been robbed, and in one instance, murdered to gain access to refund checks.

The high potential for financial gain and low physical risk have made stolen identity refund fraud the new crime of choice for drug dealers and gangs. The scope and organization of these criminals is vast and growing, and in certain cases, the criminal proceeds of the crime have been used to purchase illegal narcotics for resale.

For taxpayers who are direct SIRF victims, the economic and personal consequences can be severe and often long-term. While the IRS has invested substantial efforts and resources to address identity theft concerns, those victimized face months, if not years, of overwhelming paperwork, credit problems, and inconvenience. When a stolen identity is used to commit tax refund fraud, all taxpayers are victims, and all Americans are impacted by the loss to the Federal Treasury. In recognition of the severity of the problem, the Department and the IRS have devoted significant resources to the successful prosecution of individuals engaged in stolen identity refund fraud. Individuals engaged in this criminal conduct face a variety of charges, including aggravated identity theft, theft of government property, false claims for refund, false returns, and tax conspiracy.

In the last several years, the Department has successfully prosecuted and received significant sentences in cases in which a stolen identity was used to commit tax refund fraud. For example:

- In October 2013, in Alabama, a U.S. postal employee was sentenced to 111 months in prison for his role in a stolen identity refund scheme. The mail carrier used mailing addresses on his postal route to send debit cards loaded with false refunds. Other defendants obtained the stolen identities used on the returns from the Alabama Department of Corrections. The defendants filed hundreds of fraudulent tax returns that claimed over $1 million in false refunds.
- In May 2014, a superseding indictment was returned against nine defendants for their roles in a $20 million dollar stolen identity refund conspiracy. According to the allegations in the indictment, between 2011 and 2013, the defendants ran a large-scale identity theft ring in which they filed over 7,000 tax returns claiming false refunds. As part the scheme, one of the defendants stole identities from the hospital at Fort Benning, Georgia where she worked and had access to the identification data of military personnel, including soldiers who were deployed to Iraq and Afghanistan. Other defendants stole identities from an Alabama state agency and from the Alabama Department of Corrections.
- In June 2014, a Miami, Florida man was sentenced to 10 years in prison for stealing identities and then filing false returns that requested over $13 million in false refunds by fraudulently claiming gambling income and withholding from the Florida Lottery Commission. His co-conspirator opened approximately eighteen bank accounts to deposit these fraudulent refunds.
- In December 2014, a Tennessee woman was sentenced to 102 months in prison. She and her co-conspirators unlawfully obtained personal identifying information of victims, including high school students, and used the information to file false tax returns claiming millions of dollars of refunds. Two co-conspirators have been sentenced to 45 and 48 months in prison, respectively, and three others have pled guilty and await sentencing.
- In January 2015, a Maryland woman and former bank employee, was sentenced to 87 months in prison for her role in a massive and sophisticated identity theft and tax fraud network involving more than 130 individuals. She is among approximately a dozen people who have pleaded guilty in the U.S. District Court for the District of Columbia to charges in one of the largest prosecutions to date involving the use of stolen identifying information. The overall case involves the filing of at least 12,000 fraudulent federal income tax returns that sought refunds of at least $40 million.

As these examples illustrate, SIRF crimes are different from the crimes typically addressed by the Tax Division. While the typical criminal tax case may involve willfully filed false returns, evading the assessment of tax due and owing or the use of sophisticated financial schemes which invariably require lengthy in-depth investigations, SIRF crimes generally involve garden variety theft and fraud. Moreover, SIRF prosecutions are often reactive to exigent circumstances; in many cases, the crime is discovered by local law enforcement officers who come upon a large cache of Treasury checks or debit cards loaded with fraudulent tax refunds.

Recognizing these fast-moving law enforcement needs, on October 1, 2012, the Tax Division issued Directive 144, which delegates to local United States Attorneys' Offices the authority to initiate tax-related grand jury investigations in SIRF matters, to charge those involved in SIRF crimes by complaint, and to obtain seizure warrants for forfeiture of criminally-derived proceeds arising from SIRF crimes, without prior authorization from the Tax Division. The Tax Division retains authority in connection with forfeitures if any legitimate taxpayer refunds are involved.

Directive 144 was the result of collaborative efforts among the Tax Division, the IRS, and the United States Attorneys' Offices to strengthen the law enforcement response to SIRF crimes. The Tax Division continues to work closely with the IRS and United States Attorneys' Offices across the country to ensure effective information sharing and investigative cooperation as permitted by law. And this approach is yielding significant results. Beginning with the implementation of Directive 144 (and the expedited review procedures) and ending December 31, 2014, the Tax Division has authorized more than 975 SIRF investigations involving more than 1,700 subjects. As a result, during the same period the Tax Division and the U.S. Attor-

neys' Offices have brought more than 725 prosecutions involving more than 1,400 individuals.

The prosecution of SIRF crimes is a national priority, and, together with our law enforcement partners, we will continue to look for the most effective ways to bring this conduct to an end and to punish these wrongdoers. Indeed, enforcement efforts are critical, but the goal is to stop fraudulent refunds at the door. In the meantime, the Tax Division will continue to prosecute these cases and, in doing so, send a clear message to those who engage in this conduct that they will be held accountable for their actions.

Thank you for the opportunity to provide the Department's perspective on this issue, and I look forward to answering any questions that you may have.

PREPARED STATEMENT OF HON. ORRIN G. HATCH,
A U.S. SENATOR FROM UTAH

WASHINGTON—Senate Finance Committee Chairman Orrin Hatch (R–Utah) today delivered the following opening statement at a committee hearing on tax schemes and scams:

The committee will come to order.

The committee meets today to hear about growing criminal activity that is targeting taxpayers across the country. These criminal acts are perpetrated by thieves hiding behind telephone lines and computers, preying on honest taxpayers and robbing the Treasury of tens of billions of dollars every year.

This must stop, and we are here today to hear from some of the federal and state officials on the front lines of the fight to catch these crooks and protect taxpayers.

But first I want to talk about one case in particular, and one very large number. In this town—and especially right here on this committee—we often talk in hundreds of millions, billions, or even trillions of dollars. Some joke about a number being referred to as budget dust, even if the number has nine or ten zeros behind it.

But let me tell you about a number that is truly stunning: $15,800.

That's $15,800 saved through hard work, sacrifice, and honest living.

That's $15,800 saved for the down payment of a new house for a growing family.

And, that's $15,800 in savings that was wiped away by criminals who use fear, confusion, and intimidation as their weapons.

This is the story of the Degen family from Taylorsville, Utah, and I would like to play a news clip from KTVX, a Utah ABC affiliate, that tells their story.

This is just one family, out of millions that have been targeted and thousands that have been victimized. And this is just one scam.

But, make no mistake, taxpayers across the country are also facing identity theft in record numbers, account takeovers, and other criminal attacks.

Once again, this must be stopped.

Taxpayers must be more aware of the risks and better protected from attack. And these criminals must be found and brought to justice. I look forward to the testimony from our witnesses on today's panel and to hearing more about how we can accomplish these goals.I'll now turn it over to Senator Wyden for his opening statement.

PREPARED STATEMENT OF ELLEN M. KLEM, DIRECTOR OF CONSUMER OUTREACH AND EDUCATION, OFFICE OF THE ATTORNEY GENERAL, OREGON DEPARTMENT OF JUSTICE

Good morning. I'd like to begin by thanking Chairman Hatch, Ranking member Senator Ron Wyden and members of the Committee for allowing me the opportunity to testify today. My name is Ellen Klem and I am the Director of Consumer Outreach and Education for Oregon Attorney General Ellen Rosenblum. My job is to travel the state educating Oregonians on how to be savvy consumers and avoid being scammed by scammers and fraudsters.

Every week, I'm in a different city talking to a different group of Oregonians. For example, last week I was on the northern Oregon coast in Astoria, Oregon with Attorney General Rosenblum talking to a group of older Oregonians at the Clatsop Retirement Village, and next week I will be in Albany, Oregon talking to a group of retired teachers.

Every day, I hear stories from our most vulnerable citizens about a wide variety of scams and frauds. To an unassuming Oregonian, these scams can be threatening, and quite frankly, scary. While fraudulent behavior, imposter phone calls and unofficial mail solicitations have always been a part of a scammer's repertoire, today's scammers use new tactics.

Lately, my conversations with Oregonians have focused almost exclusively on the IRS imposter scam. This is a major headache for too many Oregonians. Looking to take advantage of people during a busy tax season, these scammers tell victims over the phone that they owe money to the IRS or Oregon Department of Revenue. The caller demands that the person pay the money immediately through a temporary debit card or a wire transfer. If the victim refuses to pay, they are threatened with arrest, deportation or suspension of a business or driver's license. In many cases, the caller becomes aggressive and insulting. For a vulnerable Oregonian, this phone call can be devastating.

In 2014, the IRS imposter scam topped Oregon's list of consumer complaints. Last year, 1,340 Oregonians filed complaints with the Oregon Attorney General about this scam, nearly double the complaints as the next highest category. Victims of this scam reported losses totaling $77,137.09. Unfortunately, we know this is just the tip of the iceberg. Many scam victims do not even report their losses because they either don't know whom to report to or are too ashamed that they have been scammed. For countless others, they may not even know they have been scammed.

That is why I am here today; to bring you the voices of Oregonians who have lost money, time and a sense of security because of these scammers. In particular, I would like to tell you the stories of two of those victims and share what the Oregon Attorney General is doing to prevent this from happening to others.

The first story I would like to share is that of a victim I'll refer to as Diane. Last year she fell victim to the IRS imposter scam to the tune of $15,000, the largest loss reported to the Oregon Department of Justice in 2014. Diane, a woman in her late 50s, lives and works in Turner, Oregon, a small town with fewer than 2,000 residents. On August 12, 2014 she received a message on her answering machine from a man claiming to be from the IRS and directing her to call him back at a Washington, D.C. phone number. She dutifully called him back and the person who answered her call proceeded to read her an affidavit for her arrest, threatened her with a fine of $25,000 and 18 months in prison, and told her she would be arrested later that day if she did not pay. Needless to say Diane was terrified. She feared for her job and her financial future, and begged for forgiveness. The scammer told her it was possible to settle the matter, but only if she paid $15,000 immediately by purchasing a pre-paid debit card at a local store. Hoping to avoid prison, and afraid of further consequences, Diane made the only choice she thought she had; she complied with the request—and she was out $15,000.

Individuals like Diane who send money to the scammers aren't the only victims of imposter scams. In September 2014, I was contacted by Marissa Phillips, a small business owner outside of Portland, Oregon whose employee, Linda, had fallen victim to an imposter scam. After sending a small amount of money to the scammers, Linda realized her mistake and stopped answering the phone. But the scammers refused to give up. They kept calling. And, when it was clear that she wasn't answering the phone, the scammers began calling Marissa's small business; a business that provides in-home services for seniors and persons with disabilities. When Marissa called me, she reported that the scammers had called her business at a rate of 100 phone calls per minute for 20 minutes; that's 2,000 phone calls in less than half an hour. All the calls from scammers prevented the small business from providing help to those that actually needed it. The seniors, their families, hospitals, doctors and other staff could get nothing more than a busy tone when they called for assistance. Ultimately, the business was forced to change its phone number, and all of its marketing materials, incurring a significant cost.

While this scam can seem daunting, thankfully not everyone in Oregon who receives a phone call from an IRS imposter will fall victim to the scam. I'd like to think that's because we have been working so hard to educate all Oregonians, especially our most vulnerable.

The Oregon Attorney General has several educational tools aimed at scam prevention, because she and I both know that well-informed Oregonians are more likely to recognize fraud and less likely to become victims. We also know these scams can be hard to track and prosecute.

Because education is so critical, we have a number of resources available for consumers, including:

- A brochure with ten tips to protect you and your family from scams,
- A toll-free complaint hotline that is staffed 5 days a week with some of the most knowledgeable volunteers in the state,
- An easy to remember website—*www.oregonconsumer.gov,*
- A searchable online consumer complaint database called Be InfORmed, and
- Scam Alerts sent via email, our website, and Twitter.

But our educational efforts do not stop there. We also have an entire section of the Oregon Department of Justice devoted to financial fraud and consumer protection.

The 34 employees of the Consumer Protection & Financial Fraud section received 50,000 phone calls in 2014 alone and receives nearly 8,000 written consumer complaints every year. Last year alone, this section opened more than 80 formal investigations and, at any given time, they are working on 220 open investigations.

That is why we have also invested in strong partnerships with federal, state, and local government entities and officials, tribes, community organizations, advocacy groups, and members of the media. Through these partnerships we're able to share complaints, coordinate investigations, and disseminate information to the public. Our partners give us a bigger voice to share information and keep Oregonians safe.

In fact, one of our most successful partnerships is the Social Services Fraud Working Group, which meets monthly. The work group—in existence since 2011—is multidisciplinary and comprised of more than 30 federal, state, and local agencies working fraud cases in the field of social services. At each meeting, members of the work group share tips and work collaboratively to fight social services fraud. The success of the work group has spawned two additional workgroups, one in Alaska and another in Washington state.

Unfortunately, Oregon is not unique in the number of reported scams. IRS imposter scam complaints are up nationally. Scammers target everyone, but especially older adults and other vulnerable individuals; they will not stop until they are caught and brought to justice. Unfortunately, that proves to be a challenge.

We look forward to continuing our collaboration with the IRS, the FTC, and other federal agencies like the Office of the Inspector General of the Social Security Administration that hosts our Social Services Fraud Work Group.

This concludes my testimony. Again, thank you Chairman Hatch, Ranking member Senator Ron Wyden and members of the Committee for inviting me today. I am available to answer questions.

PREPARED STATEMENT OF HON. JOHN L. VALENTINE, CHAIRMAN,
UTAH STATE TAX COMMISSION

Mr. Chairman and esteemed members of the Senate Finance Committee, I come before you this morning to discuss and recommend actions that can be taken to reduce the contagion of tax fraud which is sweeping the country.

There are four issues for your consideration this morning:

1. Strengthen information sharing between the IRS and the States.
2. Stricter regulation of the financial industry as it relates to "pre-paid" debit cards.
3. Prohibit the practice of applying refunds to payment of fees for filing services, a practice sometimes called "Refund Transfer."
4. Require third party filing services to tighten front end security by using multifactor authentication and other measures to secure data from unauthorized disclosure and identity theft.

Prior to the commencement of the 2015 filing season, Utah installed a state of the art computer software system to identify potentially fraudulent returns. On January 20 of this year, the Utah Tax Commission opened filing of income tax returns and deployed this system. As we began to process returns, our system started sending out verification letters to taxpayers whose returns appeared suspicious. Within ten days of the opening of the filing season, we began receiving calls from taxpayers who had received our communication about their return; they had not yet filed their returns.

We initially thought these were isolated incidents, but they were not. As that week progressed, our software identified more and more suspicious returns. We found several factors that were the same in all the suspicious returns:

- All the suspicious returns had the direct deposit information changed from the previous year's bank account to prepaid debit cards, often Green Dot brand debit cards.
- All the suspicious returns contained routing and account numbers that differed between the federal return and the state return.
- Most of the suspicious returns appeared to have the exact 2013 tax return data populated to the fraudulent 2014 return.
- The address on the suspicious returns was the same as the address on the 2013 return.
- Since most of these filings were being made through the Turbo Tax system, it appeared that something in their process was compromised.

After communicating with the owners of Turbo Tax, (Intuit), and notifying other states through our national organization, we notified the Internal Revenue Service of the possible compromise of the Modernized Electronic Filing (MEF) systems. The accounts in question were immediately sent to the IRS for review. On February 10, 2015, we sent 31 returns to the Ogden IRS Service Center that we had verified by contact with the taxpayers as being fraudulent. As of the date of this testimony, the IRS has not contacted us with the results of any determinations on their part of the nature of the returns. They did inform us in a phone conversation that they had known about a filing scheme which took a previous year's return and copied it into a current year's filing. The IRS representative stated that they had known about this scheme since last year, but had not notified the states of this fact.

Many have asked what action was undertaken by the state of Utah when it discovered this attack. In short, we hurried.

- We stopped all refunds until we could analyze the magnitude of the problem.
- During the first week, we identified five different repeating fraud schemes.
- We identified the returns with specific characteristics that were potentially fraudulent.
- We deployed our identity quiz system and commenced sending "ID verification letters" on the returns that met the unique characteristics of potential fraud.
- If the taxpayer failed the quiz, they were instructed to send us certain documentation to verify their identity, that included:

  Two forms of identification such as SSA card, passport, drivers license, state ID card, government issued photo ID, utility bill, bank statement, payroll stub, college transcript or insurance policy, and

  One picture ID.
- If the taxpayer does not respond to the quiz or fails to provide the needed information, the system will reverse the return as though it had not been filed.
- To the extent we could identify them, refund deposit requests to pre-paid debit cards have been converted to a paper warrant (check) and sent to the taxpayer's address.

As we continue to prevent the outflow of fraudulent refunds, we found great difficulty in determining the nature of financial institution routing and account information. We specifically found that there was no uniformity in numbering to distinguish traditional checking accounts and savings accounts from prepaid debit cards. For example, a prepaid reloadable debit card sold by Green Dot, appears to be linked to a bank account even though the debit card had no actual checking or savings account associated with it. (These cards may even appear as a Visa or Master

Card.) Quoting from their card holder's agreement: "Your card is a prepaid debit Visa or MasterCard card, which means that you must add funds or 'load' your card in order to use it. There is no credit line associated with your Card." Once the funds are transferred to such cards, they cannot easily be traced or recovered, a perfect vehicle to commit fraud. A simple fix would be to require a different series, letter or additional numbers to distinguish these cards from cards connected to bank or credit union checking and savings accounts.[1]

To obtain a Green Dot re-loadable prepaid Visa or MasterCard debit card, a customer is required to provide their name, address, date of birth, Social Security number, phone number, and other information that will allow Green Dot to identify customers.[2] If a Green Dot customer is pretending to be someone else by assuming that person's identity, then the identity thief has successfully obtained a fraudulent method to gain access to resources or other benefits in that person's name without the use of a traditional bank account. Perpetrators then use these fraudulently obtained pre-paid debit cards to make thousands of dollars' worth of retail purchases, quickly cash them out or drain them at an ATM. Prepaid debit cards appear to be preferable to fraudsters because the identity thief doesn't have to bother with banks, credit unions or check-cashing stores that may become suspicious when one person starts bringing in multiple tax refund checks to be cashed or deposited.

While we progressed though the investigation, we found a practice that enables fraudsters to perpetrate fraud without having anything at risk, a practice called "refund transfers." Here is how it works: The fraudster is allowed to deduct the third party filing fees from the refund. The third party filing service gets paid, the fraudster receives the refund and the state and federal government (and potentially the taxpayer who may actually be entitled to a refund) are out the funds.

Finally, we found third party filing services often lack the front end security measures necessary to protect their users in this cyber world. At a minimum, these services should install multi-factor authentication to assure that a person filing a tax return is indeed the person identified on the return. Quality fire walls and other data protections are a given, but since we are uncertain at this time of how the prior return information was obtained, it is a careful company, concerned about their product and its customers, that will invest the funds necessary to protect their data from cyber thieves.

Unfortunately, prepaid debit cards cannot be specifically identified by routing numbers or bank account numbers using the present standardized methods. A standardization of routing or account numbers to include identification of prepaid debit cards would facilitate evaluation of suspicious filers and enhance the ability of Federal and State taxing authorities to deny refunds to the fraudsters and catch fraudulently filed income tax returns.

PREPARED STATEMENT OF HON. RON WYDEN, A U.S. SENATOR FROM OREGON

Since the day the IRS opened its doors, scam artists have been hatching up slick new ways of stealing taxpayer dollars from the Treasury. What's new is, they're now stealing Americans' identities and personally threatening them on an industrial scale, while directly robbing them of their hard-earned money. The fraudsters dream up new tactics and milk them for all they're worth before they start getting caught. Then it's lather, rinse, repeat. Onto the next scam, always one step ahead of the law.

Today the committee will closely examine several of the fraudsters' latest strategies that are plaguing taxpayers. The one that's hitting my home state of Oregon hardest is the fake phone call demanding money or personal information on behalf of the IRS. In fact, these calls were the number one consumer complaint registered with the Oregon Department of Justice last year. Not everybody knows the IRS simply does not cold-call people making demands or threats. So it's pretty clear from my vantage point that there's a lot more work to be done taking on this scourge.

---

[1] An ABA routing transit number is a nine digit code which identifies the financial institution on which it was drawn. It was originally used to facilitate sorting, bundling, and shipment of paper checks back to the drawer's (check writer's) account. As new payment methods were developed (ACH and Wire), the system was expanded to accommodate these payment methods.

[2] Green Dot maintains that it is compliant with Federal money laundering laws and with all Patriot Act elements.

Given the sophistication of this criminal activity and the fact that a lot of it comes from overseas, this sure looks to me like an emerging type of organized crime. So the real question is, what's it going to take to root it out and put the bad actors on the sidelines? How about more prosecutions, stronger deterrents, or more cops on the beat? And what's the best way of getting the word out so that taxpayers aren't tricked into surrendering their life savings to some intimidating voice on the other end of the phone line?

But even if people manage to avoid the phone calls, you can bet the crooks are finding other ways to profit. Tax preparation software has become the scammer's new fast lane. These sharks manage to acquire a taxpayers' personal data from the black market or hack into commercial databases, and they file false returns electronically. The victims may not find out until much later in tax season, and by then it's too late. Already there have been thousands of reports like this in 2015. As we'll hear today, some software vendors aren't doing enough to help prevent fraud.

In my view, part of the challenge is getting states, Internet tax services, and the IRS on the same wavelength. Everybody's got to communicate and work together to make sure criminals can't just nimbly slide from one jurisdiction to the next, as they rip off more unsuspecting Americans.

Taxpayers may choose to avoid software, but not even a paid tax preparer is guaranteed to be safe. In fact, many of them don't have to meet any standards for competence. There are far too many con artists out there willing and able to prey on the people who come through their doors. In some egregious cases, they secretly falsify their victims' returns to boost the refunds, and they pocket the difference. And once tax season ends, the crooks disappear from the storefronts they occupied, leaving no trace of where they've gone.

A few states, including Oregon, have rules in place to help shield taxpayers from this kind of scam. But most states don't. Senator Cardin and I introduced the Taxpayer Protection and Preparer Proficiency Act at the beginning of this Congress to give all Americans the security they deserve. Our colleague Senator Nelson is also a leader on this issue of keeping taxpayers safe from identity theft and fraud. And I'm sure they share my desire to take on these challenges on a bipartisan basis.

There is no end to the ingenuity of tax scam artists. My hope this morning is that we'll get more fresh ideas for catching up to this wave of fraud and stopping it. That can't come soon enough. So I'm looking forward to talking with our witness panel here today, which I'm very happy to say includes Ms. Ellen Klem, the director of consumer outreach and education in the Oregon Attorney General's office. Thank you, Ms. Klem and all our witnesses, for being here during a time of year that's busy for all of you.

COMMUNICATION

LETTER SUBMITTED FOR THE RECORD BY OPERATION HOPE

March 11, 2015

Honorable Mike Crapo
Chairman
Senate Subcommittee on Taxation and IRS Oversight
219 Dirksen Senate Office Building
Washington, D.C. 20510

Honorable Robert P. Casey, Jr.
Ranking Member
Senate Subcommittee on Taxation and IRS Oversight
219 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Mike Crapo and Ranking Member Robert Casey:

Operation HOPE is dedicated to financial empowerment for everyone in American society, and believes deeply that the expansion of the middle class depends on financial literacy and financial opportunity for lower income people so they can improve their lives and their futures. This year marks the 9th year for the advocation of IRS Earned Income Tax Credit Awareness (EITC) by Operation HOPE. Since 2006, we have worked to promote the EITC Program and there are many challenges we face to achieve this, but among them is the potential for an additional burden that efforts to combat tax fraud may have on the most vulnerable citizens.

Cyber fraud attacks on financial systems in the United States are a major threat for our government and our institutions. But these also represent a major threat to people. The human side of financial and tax fraud is deeply concerning, not only in terms of innocent people being victimized by fraudsters, but also by being inadvertently caught up in government battle tactics as the war against fraud is waged.

The IRS Taxpayer Advocate has written in multiple Annual Reports to Congress about innocent taxpayers being victims, both coming and going, in the story of tax fraud. She specifically addressed the problems of law-abiding individuals and families whose tax refunds have been held up or frozen by Government, suffering hardship and unnecessary financial crisis. She also warns of innocent citizens having their returns incorrectly flagged for investigation as the result of imprecise or overly sensitive anti-fraud filters and screens. Her reports should serve as a warning to carefully consider tactics as we consider how to go about ridding our tax system of fraud.

There is much recent talk about imposing requirements or encouraging the tax industry to help Government by identifying and flagging suspect returns, and Government increasing its fraud defenses to stop suspicious returns, freeze refunds, and investigate filers. While effective strategies for fighting fraud do require private sector cooperation with Government, there are also inherent risks to our citizens from a tax system dominated by fear of fraud and not balanced by concern for rights. It will not be a successful strategy for private industry to voluntarily or by government order act like deputized U.S. Marshalls, effectively making "citizen's arrests." Doing so places businesses in the position of improperly investigating and reporting their customers to the IRS—essentially extending the policing powers of the government directly into the private sector.

Those working to escape poverty, as well as the underserved and the struggling middle class, deserve better than to be profiled, whether economically or by the circumstances of their lives. Those pulling themselves up the bottom rungs of the economic ladder should not be treated as a suspect class, targeted for either greater tax compliance burdens than the rest of the population, or flagged as a targeted population for tax examination and investigation. Claiming the Earned Income Tax Credit should not mark the citizen for suspicion, nor for imposition of heavier compliance burdens and costs.

In the tax context, this means we cannot embed an assumption in our voluntary compliance tax system that taxpayers should be treated as if they are guilty until proven innocent.

We know your Subcommittee will appropriately review the threat of tax fraud not only in the context of the security of our tax system, but in the necessity to avoid collateral damage to innocent people, swept up in broad and imprecise identification for investigative and enforcement activity based solely on computer algorithms.

We urge the Subcommittee to diligently examine and question both public and private strategies to satisfy itself that we stay true to our values as we combat wrongdoing. The tax industry needs rational regulations and standards on how this fight should be fought, and Government needs active oversight and accountability to ensure fairness and decency. Congress needs, through its Oversight, to ensure that we are not losing our values as we work to combat wrongdoing.

We stand ready to assist and support the Subcommittee in any way that might be helpful in your pursuit of these critical concerns on behalf of honest taxpayers, who represent the overwhelming majority of the tax a in public in this country.

All the best and . . .

With HOPE,

John Hope Bryant
Founder, Chairman and Chief Executive Officer
www.operationhope.org